



Cisco Intelligent Automation for Cloud 4.2 Administrator Guide

Release 4.2
Published: April 30, 2015



Cisco Intelligent Automation for Cloud Administrator Guide

Release 4.2

Published: April 30, 2015

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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

Cisco Intelligent Automation for Cloud 4.2 Administrator Guide

© <year> Cisco Systems, Inc. All rights reserved.



Introduction

Cisco Intelligent Automation for Cloud 4.2 (Cisco IAC) is a self-service provisioning and orchestration software solution for cloud computing and data center automation. Cisco IAC users access services and tasks using Prime Service Catalog, a browser-based interface that provides links to services and status, such as ordering servers, viewing requisitions, and monitoring system resources.

Understanding the Cisco IAC 4.2 User Interface (UI)

Modules

Modules are role-based containers of Prime Service Catalog services grouped by purpose. This section describes Prime Service Catalog modules containing services that are covered in this guide. The module drop-down list is located in the upper-right corner of the window. You use it to open any module to which you have access. Cisco IAC 4.1 is divided into Modules dedicated to particular services available to each role type include (in menu order):

- Service Portal
- Service Catalog
- Service Manager
- Organization Designer
- Portal Designer
- Service Item Manager
- Administration
- Catalog Deployer
- Service Link

Note: For more information, see [Portals / Modules, page 5](#) as well as [User Roles, page 30](#).

Portals, Portal Pages, and Portlets

Portal pages and portlets (subsets of certain portals) contain links to the order forms for services. To add, modify, or remove portals or portlets, follow these steps.

1. From the modules drop-down, choose Portal Designer.
2. You will see the Portal Designer Portal.

Note: For complete information on how to use the functionality available on this portal, please see the [Cisco Service Portal Designer Guide](#).

Portal Pages

Cisco IAC provides the following portal pages, listed in order of the Cisco IAC menu bar. When you sign in to Cisco IAC, you may or may not see this full list of portal pages. Access depends upon your role. The default home page somewhat corresponds to the Cisco IAC menu/tool bar at the top of the screen. You can set your home page to any page you want in the system at your convenience. However, we recommend that you continue to use the Cisco IAC Home Page as your default, for ease of use. Click the **Cisco logo** at the top of the page at any time to return to your Cisco IAC home page.

My Cloud

- **My Orders**—Displays the status of all your orders, whether ordered for yourself or on behalf of another user. Depending on your user role, you may also be able to see orders for all the users in the business units (Organizations) of which you are a member.
- **My Run Rate**—Displays run rate info and lets you adjust/filter the view as needed.
- **My Containers**—View and perform actions on your vCloud Director vApp VM containers.
- **My Servers**—View and perform actions on your deployed servers, including powering up or down, decommissioning, and snapshots. All users can access the My Servers portal page.
- **My VDCs**—Access to the list of VDCs, which contains the service links to Modify VDC Size, Decommission VDC, Add a Network to VDC, Remove Network from VDC, Order a VM from Template, Order a VM and Install an OS.
- **My Applications**—Displays a list of installed applications and associated Configuration Server type environment, and infrastructure information for each application. An Applications Dashboard is included for monitoring.
- **Order Services**—For ordering services.

Note: For all “My” portal pages (My Orders, My VDCs, etc.), the view is hierarchical. The CPTA can see all options. The TTA can see all orders associated with the tenant account. The OTA can see all orders associated with the organization. The VSO and VPSO can see only their orders.

Setup

- **Configuration Wizard**—Optional access to configure Cisco IAC, which contains the configuration of Agent Properties Configuration, Cloud Administration, Connect Cloud Infrastructure, POD Management, Set System-wide Services and Provisioning Settings, and Create Shared Zone.
- **System Settings**—Manage a variety of cloud resources, including data connections, server templates, networks, UCS blades and blade pools. Only Cloud Provider Technical Administrators can access the System Setup portal page.
- **Manage Infrastructure**—Access to Discovery and Manage Cloud Infrastructures.
- **VDC Calculator**—Calculate the Planned VM Distribution, Planned VM Configuration and Suggested VDC Package from Planned VDC VM Limit.

Management

- **Tenant Management**—On-board, off-board, and modify tenants.
- **Price Rates**—Set and modify price rates.

Operations

- **Approvals**—Displays approvals assigned to you directly or to your queues, and enables you to see approvals that precede or follow yours. Depending on your role, you may also be able to see approvals for orders placed by user in your business units.
- **Error Remediation**—Access to the Cloud Service Errors, which contains the service links to Error Remediation actions such as Cancel, Restart, Retry, Ignore and Rollback.
- **Network Management**—View network usage, assign, unassign, and exclude IP addresses
- **System Health**—Access to the System Health details, which contains the service links to validate the Platform Elements and validate Cisco Process Orchestrator.
- **System Resource Capacity**—View capacity information for virtual clusters, UCS blades, and chassis. Only Cloud Provider Technical Administrators can access the System Resources portal.

Site Homepage

Service Portal is the default module users see when you first log in to Cisco Intelligent Automation for Cloud 4.2. You are presented with the Cisco IAC Home Page. You access the Cisco IAC 4.2 Home Page in any one of the following ways, as you prefer:

- Click the **Cisco Intelligent Automation for Cloud logo**.
- Click the **Cisco Intelligent Automation for Cloud 4.2 title bar**.
- Click the **Home** button (looks like a house) in the upper right corner of the screen and choose Home.
- Choose **Service Portal** from the module drop-down list on the upper-right corner of the screen.

Changing Your Home Page

Follow these steps to change your home page as needed. Use these same steps to change back to the Cisco IAC default home page.

1. Navigate to the page you want to use as your workspace.
2. Click **Home Page Dropdown** button next to the module drop-down list in the upper-right corner of the window.
3. Click **Set As Homepage**.
4. Click **OK**.

Disabling Reserved Portlet Buttons

Reserved portlets are out-of-the-box portlets that ship with Cisco Prime Service Catalog which can be added to portals by clicking buttons in the toolbar in the Service Portal module. Unless you hide them, these buttons appear by default. When you click a reserved portlet button, it adds a portlet to the portal you are currently viewing. **Reserved portlets cannot be removed from a portal or edited after they have been added.** However, you can set any or all of them to “inactive” to remove the buttons from the toolbar.

1. Choose **Portal Designer** from the module drop-down list, then click the **Portlets** tab.
2. Expand **Reserved Portlets** in the left pane and click any of the portlets in the folder.
3. In the Content Portlet Information pane, click the **Inactive** radio button and then click **Save**.

4. Repeat the above steps, as needed, for other reserved portlets that you want to inactivate.

Re-enabling

To re-enable reserved portlet buttons:

1. Choose **Portal Designer** from the module drop-down list, then click the **Portlets** tab.
2. Expand **Reserved Portlets** in the left pane and click any of the portlets in the folder.
3. In the Content Portlet Information pane, click the **Active** radio button and then click **Save**.

Inactivating Reserved Portlet Buttons from the Service Portal Toolbar

There are three reserved portlets whose buttons appear by default:

Reserved Portlet Button	Description
Search	Adds a Search portlet to the current portal. It allows you to search for services by name.
Orders	Adds an Orders portlet to the current portal that displays a list of recent orders.
Approval	Adds an Approvals portlet to the current portal that displays a list of tasks needing approvals

When you click a reserved portlet button, it adds a portlet to the portal you are currently viewing.

Reserved portlets cannot be removed from a portal or edited after they have been added. However, you can set any or all of them to “inactive” to remove the buttons from the toolbar.

To inactivate the reserved portlets, complete the following steps.

1. Choose **Portal Designer** from the module drop-down list, then click the **Portlets** tab.
2. Expand **Reserved Portlets** in the left pane and click any of the portlets in the folder.
3. In the Content Portlet Information pane, click the **Inactive** radio button.
4. Click **Save**.
5. Repeat [1. Choose Portal Designer from the module drop-down list, then click the Portlets tab., page 3](#) through [4. Click Save., page 4](#) for other reserved portlets that you want to inactivate.

Portal Purpose and Location

Each portal page is located within a module according to its purpose. Portals can serve three purposes:

- **Provide information**—For example, the System Resource Capacity portal displays capacity information about your cloud resources, including UCS blades and virtual data centers.
- **Link to forms**—For example, the Tenant Management portal provides links to forms for adding or removing users, viewing and modifying organization properties, removing organization networks, and so on.
- **Provide both**—For example, the My Servers portal displays tables with specifications and editable properties of the servers under your control. It also allows you to perform several services on a server, such as powering up or down, decommissioning, and reverting to snapshots (VMs only).

Portals / Modules

Service Portal

This is the portal option for accessing the Cisco IAC 4.2 user interface.

Service Catalog Module

For accessing Cisco Prime Service Catalog.

Service Manager Module

The Service Manager module enables Cloud Provider Technical Administrators (CPTAs) to manage, assign, and track progress on tasks for Service Team members. The Cloud Provider Technical Administrator uses Error Remediation Services and Approvals portlets to try and remediate Cloud services. Only Cloud Provider Technical Administrators, Organization Technical Administrators, and site administrators have permissions to access the Service Manager module.

Organization Designer Module

Cloud Provider Technical Administrators use Organization Designer to create, modify, and remove users. Cloud Provider Technical Administrators and site administrators have permissions to access the Organization Designer module.

Portal Designer Module

Used for choosing and designing portal pages.

Service Item Manager Module

The Service Item Manager module provides tools for managing service items and ordering standards. Ordering standards are defined options that users can choose when ordering servers. For example, you can define the server sizes users can order; these options appear in drop-down lists on server order forms. Only Cloud Provider Technical Administrators, Cloud Provider Business Administrators, and site administrators have permissions to access Service Item Manager.

Administration Module

Access the Administration module to perform administrative tasks, such as editing system-wide settings, configuring authorizations and reviews, setting up notifications, and administering email templates. Only Cloud Provider Technical Administrators have permissions to access the Administration module.

Localization Module

For managing, updating, and assigning the languages used in the Cisco IAC 4.2 user interface.

Catalog Deployer Module

There is a Catalog Deployer Portal for working with catalog items.

Service Link Module

There is a Service Link Portal for accessing various management options.

Profile Settings and Preferences

You can add or update personal settings and preferences in your Prime Service Catalog user account. From the Profile portal, you can perform the following:

- Change your Prime Service Catalog password
- Add, update, or delete contact and location information
- Add, update, or delete calendar information, such as your working hours and scheduled time off
- Change personal preferences for date and time format, login module

Changes to your personal settings, such as password and time zone, automatically update your Prime Service Catalog user account. To access your profile settings, click the drop-down next to your username at the top of any page in Prime Service Catalog, then click Profile.

Customizing Table Views

In Prime Service Catalog, most table views are customizable per user. You can sort rows in ascending or descending order by column. In some cases, you can also choose which columns to show or hide. When you change the table view, your personal settings are retained unless or until you change them again, or if you have cookies disabled in your browser settings.

Re-sorting Table Rows by Column

By default, table rows are sorted by ascending order of the first column. To re-sort the rows by another column, click the column title. To re-sort the rows in ascending or descending order by column, hover the mouse pointer over the far right side of the column title until an arrow appears, click the arrow, then choose **Sort Ascending** or **Sort Descending**.

Adding or Removing Columns

Hover the mouse pointer over the **gear** icon  with the drop-down in the far right side of the table. Choose **Columns**. Then, check or uncheck boxes for any of the available columns. You can always reset the columns back to default settings.



Network Services Overview

Understanding Network Services

Bundled Technologies

Cisco Intelligent Automation for Cloud 4.2 ships with the following components.

Bundled Suite Components

- Cisco Cloud Services Router
- Citrix NetScaler 1000v (formerly Citrix NetScaler VPX)
- Cisco Prime Service Catalog
- Cisco Process Orchestrator
- Cisco UCS Manager
- Cisco Virtual Security Gateway (VSG)

Suite Components / New Integrations

- Amazon AWS (EC2)
- Chef Server
- Cisco Application Policy Infrastructure Controller (Cisco APIC)
- Cisco ASA 1000v Limited Support
- Citrix NetScaler 1000v
- Cisco Nexus 1000v
- Cisco Prime Network Registrar IPAM
- Cisco Prime Network Services Controller
- Cisco UCS Director
- Cisco Virtual Security Gateway
- OpenStack Juno and IceHouse
- Puppet Labs' Puppet Master
- VMware vCenter Server
- VMware vCloud Director

Note: For for the full list of interoperable components, see the [Cisco Intelligent Automation for Cloud 4.2 Cisco Intelligent Automation for Cloud Compatibility & Requirements Matrix](#).

Network Architecture

VSA 1.0 Design

- Orchestration of VSA 1.0 Virtual Network Services Design:

- Nexus 1000v
- CSR 1000v
- Cisco Virtual Security Gateway (VSG)
- Citrix NetScaler VPX / Citrix NetScaler 1000v

Note: Citrix NetScaler 1000V brings together Citrix NetScaler with Cisco Nexus 1000V Switch vPath technology for policy-based service insertion and chaining. As of Citrix NetScaler 1000V Release 10.1-124.14, vPath can be disabled to load-balance physical servers or load-balance workloads running on any hypervisor. Note that Cisco IAC no longer uses vPath for NetScaler, but only for VSG.

VSA 2.3 Design

- Extendable to support VSA 2.3 Design:

- ASR 1000
- Cisco 7600
- Nexus 2000/5000/7000
- ASA-SM
- FWSM
- Extensible to additional devices and architectures

Supported Virtual Appliances

Cisco IAC 4.2 Virtual Appliances and their functions are listed below.

Table 1 Virtual Appliances

Appliance	Function
Citrix NetScaler 1000v	Virtualized load balancing per Tenant's Organization
CSR 1000v	Virtual routing instance Hypervisor-isolated, Virtual enterprise-class Cisco IOS-XE router per Tenant's Organization. Used primarily for zone-based firewall capabilities.
Nexus 1000v	Distributed vSwitch
Prime NSC	Dynamic, template-focused network policy management based on service profiles for Security Policy Management. Tightly integrated with management and orchestration tools such as Cisco IAC 4.2.
Virtual Security Gateway (VSG)	Virtual zone to secure intra-network traffic.

Note: For for the full list of supported Virtual Appliances, see the [Cisco Intelligent Automation for Cloud 4.2 Cisco Intelligent Automation for Cloud Compatibility & Requirements Matrix](#).

Platform Elements and POD Relationships

The table below shows the relationship information between specific platform elements and PODs.

Table 2 Elements and PODs

Platform Element	# of PODS	POD Information
Chef Servers	0+	Can only be used by one Service Resource Container at a time; in other words, there is only a 1-1 relationship between a ChefPE and the Service Recourse Container.
Cisco APICs	0+	Can only associate with a Cisco APIC-enabled OpenStack Cloud Manager deployment. For more information on Cisco APIC and OpenStack, see http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/api/openstack/b_Cisco_APIC_OpenStack_Driver_Install_Guide.html
Cisco Nexus 1000vs	0+	Networks must be pre-provisioned if no Nexus 1000v is registered
Cisco Prime Network Registrar IPAM	0 or 1	Only one may be associated to a Compute POD
Cisco Prime Network Service Controllers (PNSC)	0+	Only one may be associated to a Service Resource Container
Cisco Prime Service Catalog	1	One or more in the web tier and database tier; one in SL tier
Cisco Process Orchestrators	1+	Platform Element associated with PSC for service fulfillment.
Cisco Unified Computing System (UCS) Director	0 or 1	One may service multiple Network PODs
Cisco Unified Computing System (UCS) Manager	0+	Only one may be associated to a Compute POD
Cisco Virtual Security Gateways	0+	Two VSGs per Nexus 1000v per Tenant Organization, although one per organization is typical; two in HA. (Choosing HA is possible and two will be deployed but will not be fully configured for HA for Cisco IAC 4.2.)
Citrix NetScaler 1000v	0+	One Nexus 1000v per many Citrix NetScaler 1000v per Tenant Organization
Cloud Service Router (CSR) 1000vs	0+	There can be only one VSG, CSR, and NetScaler per Organizations but multiple Organizations per Tenant.
OpenStack Cloud Managers	0+	Associated with Compute PODs referencing Network PODs. Note that multiple Compute PODs are possible.
Puppet Labs' Puppet Master	0+	Can only be used by one Service Resource Container at a time; in other words, there is only a 1-1 relationship between a Puppet PE and the Service Recourse Container.
VMware vCenter Servers (not Linked mode)	1+	One or more may be associated to a Compute POD.
VMware vCloud Director	0+	Multiple compute pods are possible.

Use Case by Persona

Cloud Provider Technical Administrator (CPTA)

Set Provisioning (Add Networks, Public Subnet)

- Connect to managers and devices
- Discover and inventory virtual and physical network devices
- Discover and define network topology (device interconnects)
- Perform network device connectivity checks
- Manage network device credentials
- Define, update and remove Network PODs
- Associate to Compute PODs
- Add Cloud Admin Users
- Approves Create VDC etc. requisitions
- Error Remediation privileges

System Settings and Behavior

- Define Internet and Enterprise routing behavior
- Define IPAM authority for network provisioning
- Identify virtual network appliance images

Greenfield/Brownfield Support

- Support Greenfield Network PODs
- Coexist with Brownfield networks and services for existing tenants (enabling migration)
- Perform discovery of existing networks by discovering available and used IP addresses

Tenant Management

- On-board new tenants and organizations and set up initial network services
- Off-board existing tenants and organizations and remove all network resources
- Modify Tenants and Organizations

Ongoing Management

- Network inventory synchronization (manual invocation)
- Display utilization of system network resources (networks, policies, and so on)
- Views for capacity management of VDCs
- Views for capacity management of tenant network resources (private cloud case)

Use Case by Persona

- View ordered networks and network services by tenant

Application Management

- View the applications installed
- View consumption rates

Cloud Provider Business Administrator (CPBA)

Service Management

- Set master pricing of cloud services and cloud resources
- Virtual Machines (and resources)
- Virtual Data Centers (sizes)
- View all or tenant-specific prices and run rates

Tenant Management

- Onboard new tenant with or without tenant-specific discount
- Set tenant-specific service offering elections

Application Management

- Application consumption rates

Tenant Technical Administrator (TTA)

View

Available network services offered by the cloud provider

Choose

- Choose network services to be offered to tenant users.

Order

- Order tenant-level resources (shared network zone, public IP pool, etc.)

Manage

- Access to different organizations
- Access to the same VDC (share private VDCs)
- Define network tenant firewall and load balancer service groups
- Define tenant network security policy
- View VDC, network, and tenant services ordered by tenant users
- Monitor resource utilization of tenant network resources

Organization Technical Administrator (OTA)

View

- Available organization VDCs and other resources

Order

- A VDC, choosing size, zones, and networks for the organization

Manage Lifecycle

- Modify VDC zones and networks
- Add, modify, or remove NAT, server firewall, server load-balancing
- Manage server and service groups
- Decommission VDCs

Server Owner / Application Architect

- Order servers
- View accessible VDCs and shared zones and their resources
- Use static or dynamic IP addressing
- Manage individual server firewall and load-balancer service policy
- Manage individual server membership to server and service groups
- Single or bulk server deployment: Deploy multiple virtual servers of the same type

Understanding Server Groups

A server group is a collection of servers which may be used as source or destination endpoints. (Not to be confused with the service group concept in PSC Service Designer module.) Server Groups are logical collections of related servers on the same network. Server Groups are used to apply and define firewall services and policies. Server Groups are based on IP addresses, which are applicable to both physical and virtual servers. In addition, servers can be added and removed from Server Groups without having to create/modify/delete any firewall or load balancer rules. Firewall rules that target Server Groups use the source or destination qualifier.

Understanding Service Groups

Service Groups (not to be confused with the *Service Design* term or object or with *Server Groups*) are a collection of port, protocol, and monitor combinations that can be used as a single manageable entity for firewall and load balancing purposes. Service Groups offer application and management of policy broadly across associated servers and server groups. There are two types of Service Groups: Firewall Service Groups and Load Balancer Service Groups.

Load Balancer Service Groups

Cisco IAC 4.2 ships with a default set of Load Balancer service groups for HTTP, HTTPS, and SSL Offload.

About SSL Offload

SSL Offload leverages the benefits of VPX SSL Offloading feature by offering this capability through an orderable service in the Prime Service Catalog (PSC) when configuring a VPX Load Balancer. An SSL virtual server and a service group get configured on the VPX appliance. SSL traffic will be offloaded to VPX from having to be processed by the web servers. This way VPX can handle the CPU-intensive SSL encryption/decryption of the client traffic on behalf of the servers.

Load Balancing Service Groups

Load balancing service groups distribute network traffic between a group of servers. End users will choose from a VIP that is designated with SSL which will indicate that secure web traffic will be offloaded from having to be processed by the actual web server. SSL OFFLOAD will have VPX do SSL offloading and handle encryption/ decryption on its behalf.

Configuring SSL Offloading in Cisco IAC

- A new service group template, SSL OFFLOAD, is created in a standards table on PSC.
- From a service group template a service group instance will be created and bound to an SSL virtual server.

Note: You order a VPX Load Balancer using SSL Offloading service group template in Cisco Prime Service Catalog (Management > Tenant Management).

VPX Concepts

- **SSL Virtual Server:** Load-balancing virtual server of protocol type SSL. Intercepts SSL traffic from clients, decrypts it and processes it before sending it to services that are bound to the virtual server.
- **Service:** A server or an application on a server. For an VPX appliance to forward decrypted SSL data to servers in the network, services must be bound to a virtual server that receives SSL data.
- **Service Group:** Logical aggregation that enables the management of a group of services as a single service. If you enable or disable any option for a service group, the option gets enabled for all the members of the service group. After creating a service group, you can bind it to a virtual server, and you can add services to the group.

About VPX SSL Offloading

SSL offloading feature ensures secure and performance delivery of web applications by offloading CPU-intensive SSL encryption and decryption tasks from the local web server to the VPX appliance. To configure SSL offloading, a virtual server gets configured to intercept and process SSL traffic, and send the decrypted traffic to the server. Upon receiving the response from the server, the appliance completes the secure transaction with the client. From the client's perspective, the transaction seems to be done directly with the server.

Lifecycle of Load-Balancer Service Group

When on-boarding an organization, the set of service groups is inherited from the provider-defined global set. Provider may modify the target global set at any time. New Tenants receive the default Provider settings upon on-boarding. In addition, an Organization inherits from the service groups defined by the TTA when on-boarded. Note that new service group additions are not propagated to existing Organizations. Also, when on-boarding an organization, a default set of service groups is inherited from a Provider-defined global set.

Firewall Service Groups

Cisco IAC 4.2 ships with a default set of Firewall service groups:

- Database (Microsoft)
- Database (MySQL)
- Database (Oracle)
- Database (PostGRES)
- FTP
- Remote Access

- Web

Life Cycle of Firewall Service Group

A provider may modify this default set at any time. An Organization receives this default set upon on boarding. Again, as with Load Balancer service groups, new service group additions are not propagated to existing Organizations. When an organization is on-boarded, a default set of service groups are inherited from a Provider-defined default set.

Firewall Rules

Firewall rules meta data is captured in a method that is technology-agnostic. Rules are applicable to Cisco Virtual Security Gateway (VSG) and Cisco Cloud Service Router (CSR), and are stored in designated Firewall Policy Rules.

Network Topologies

Cisco IAC 4.2 includes a base set of sixty (60) VDC zone-based topologies. Additional permutations are possible based on the number of networks per zone.

The 60 permutations are based on variations of:

- Level of Service:
 - Gold
 - Silver
 - Bronze
- Connectivity Type:
 - Internet
 - Enterprise
 - Both

and

- Tenant Network Zone Type:
 - Unprotected Public
 - Protected Public
 - UnProtected Private
 - Protected Private)

VDC Topology

The table below shows the VDC topology by zone type.

Zone Type	Public IP Space	Private IP Space	Inter-Zone Firewall	Intra-Zone Firewall	Inbound Static NAT (floating IP)	Dynamic NAT
Unprotected Internet	Yes	No	Yes	No	No	No
Unprotected Enterprise	No	Yes	Yes	No	No	No
Protected Internet	No	Yes	Yes	Yes	Yes	Yes
Protected Enterprise	No	Yes	Yes	Yes	No	No

Points of Delivery (PODs)

There are multiple POD (Point of Delivery) types for Cisco IAC 4.2:

- Compute POD
- Network POD
- Service Resource Container

Compute PODs let you to specify compute infrastructure. For example, in the case of the Cloud Infrastructure Type, VMware vCenter Server, the Compute Pod has selections for Network Pod, vCenter instance, DataCenter, UCS Manager, as well as Physical Server Provisioning selections. They work together to associate and assemble Compute and Network Resources.

Compute POD

Cisco IAC 4.2 models these Compute PODs so it understands how it is that various infrastructure is associated to other infrastructure, so it can empower the cloud administrator with common tools of capacity management of that infrastructure.

Network POD

Cisco IAC 4.2, the network POD allows you to define and select network resources (VLANs, devices, etc.) to be able to be referenced by the Compute POD and, ultimately, by the Service Resource Container.

Service Resource Container

Provides a container for the infrastructure of network services offered to tenants. The SRC has selection of Compute POD which will determine the data center. A selection of cluster and data store is made available. Networks such as Infrastructure, Service and Internet Transit are also available if Advanced Networks Services is enabled globally.

Points of Delivery (PODs)



Managing Services

Viewing Service Requisitions

View service requisitions that you ordered for yourself and for others, status of each request, see error details, and track how close it is to completion. See also Order Status Portlet documentation in the [Cisco Service Portal Designer Guide](#).

1. Choose **My Cloud > My Orders**.

The Order Status portal displays your order information, such as Requisition ID, Tenant Name, Order Date, and so on.

2. Choose the orders that you want to view.

Note: You can choose to view all of your orders or choose based on the status of the service requests. You can filter to view the orders based on progress or by Requisition ID.

3. Click the triangle (▶) to view the details of the service and the percentage of completion.
4. Use the **gear** icon ⚙ to hide columns as needed.
5. Close the window when you are done viewing the details.

Managing Server Leases

A server lease is a time period after which an active server is automatically decommissioned. Leases are optional and can be set when you order a server. Server leases are optional. At the end of the lease term, the server is decommissioned automatically. There are two successive expiration dates:

- **Lease Expiration**—The server is powered down—but not deleted. Any stored data is preserved but cannot be accessed by users unless the lease is extended.
- **Storage Lease Expiration**—The server is permanently deleted and any stored data is lost.

Notifying a User of Approaching Lease Expiration

Cisco IAC provides two customizable email notification templates for notifying a user of an approaching expiration date:

- Lease Expiration - First Warning
- Lease Expiration - Second Warning

Note: Only CPTAs can extend a lease after expiration. CPTAs can extend the lease within the window where the lease has expired but before VM is decommissioned.

You can choose when each email notification is automatically sent. To view and modify the Lease Expiration - First Warning template for a user's organization, see [Managing Email Templates, page 84](#).

Note: Timing for emails is generally controlled by the service plan (or in some cases PO). It is not controlled where the manage email template link leads to.

Viewing Server Lease Information

View the expiration and storage expiration dates of a lease on a server from the My Servers portal page.

1. Choose **My Cloud > My Servers**.
2. On the My Servers portal, locate and click the server in the table.
3. Lease information is shown in the Details section for the chosen server.
4. Click the server line again to hide the details.

Note: My Servers is one of the few views without the arrow/triangle control to show and hide the details. So, you instead click on the row to show and again to hide.

Extending or Removing a Server Lease

Extend the expiration date on which a server is decommissioned but is not deleted. You can extend a lease during the lease term or after lease expiration but before storage expiration. You can also remove an existing lease from a server without deleting or decommissioning it. By removing a lease, you are simply stopping the automatic decommission service.

Note: When extending a lease, the start date is not the end of the previous term, but the date of the extension submittal.

1. Choose **My Cloud > My Servers**.
2. On the My Servers portal, locate and click the server in the table. Details about the server and icons for actions appear in the Take Action area.
3. Click the **Extend Lease** icon to open the Extend Managed Lease Instance form. The name of the server and its expiration date appear on the form.
4. From the **Term** drop-down list on the Extend Managed Lease Instance form, choose the number of days you want to add to the lease term (starting with the change date, not the end of lease date), or choose **No Lease** to remove the lease from the server.

No Lease	6 months
30 days	9 months
90 days	1 year

5. Click **Submit Order**.

Managing Infrastructure

Cisco Intelligent Automation for Cloud 4.2 includes a number of ways to manage your infrastructure.

Maintaining Your Servers

A multitude of actions are available based on the permissions for your role, these include server operations such as decommissioning VMs, to lifecycle management, such as extending a server lease. You can view your servers as well as act on them at any time. To do so:

- **My Cloud > My Servers**.

Note: For information on managing bare metal and blades, see [Managing Bare Metal and Blade Pools, page 123](#).

Infrastructure Ownership Reassignment

There will be times when you need to change ownership of a virtual server to another user. Typical scenarios include changing ownership to a support person for repairs and upgrades, and then switching ownership back to the original owner. Another example would be if an employee assigned to a VM is no longer available, you can reassign that VM to a different employee.

Note: You can only reassign ownership to another user within the *same* organization. To reassign ownership (typically the task of an Organization Technical Administrator, start at the drop-down menu.

1. Choose **My Cloud > My Servers**.
2. Choose the device for which you want to change ownership.
3. Click the **gear** icon  next to the server name.
4. In the popover, click the “Modify server ownership” icon.
5. The Modify Server Ownership form displays.
6. Click **Choose** to open the Choose Person form.
7. Search for the person to reassign this server to (wildcards such as **?** and ***** are acceptable; for example DE*).
8. From the list that then displays, click the radio button for the person you want to use, then click **OK**.
9. Click **Submit**.
10. Close the information form showing you that the request has been completed.
11. Close the popover.

Using the Managing Infrastructure Portal

1. To access this portal, choose **Setup > Manage Infrastructure**. You will see the Manage Infrastructure portal display.
2. Choose any of the buttons on the left side to access information on:
 - Amazon EC2
 - Chef
 - Cisco IAC Management Appliance
 - Cisco UCS Director
 - Cisco UCS Manager
 - Cisco Prime Network Services Controller
 - Network Elements
 - OpenStack
 - Puppet
 - VMware vCenter Server
 - VMware vCloud Director

Note: As you click on any of the above, the area beneath that button expands, displaying a clickable list of items for you to choose from. In addition, the graphs and tables to the right change.

3. Choose an item to analyze the information.
4. Continue with another network device type.
5. Close when done.

Checking System Health

You can check system health at any time. You can also opt to turn on or off automatic health check.

Note: Via Prime Performance Manager (PPM), asynchronous alarms persist in the page header area on every page/screen in the program.

Turning Automatic Health Check On or Off

Access the Set Provisioning Settings Form this way (starting at the modules selection menu in the upper right of the screen):

1. **Setup > System Settings > System Settings.**
2. Click **Set Provisioning Settings.**
3. On the Set Provisioning Settings form, you will notice the System Health Check option.
4. From the drop-down, choose the state you want Health Check to be in:
 - Off / **On** (default)
5. Click **Submit Order.**

Viewing System Health

To view the current status of your systems' health, use the Set Provisioning Settings Form this way (starting at the modules selection menu in the upper right):

1. Choose **Operations > System Health.**
2. On the System Health Status page, view and manage your systems' health. Cisco IAC only displays those platform elements that have been onboarded to your environment.

Note: Notice the Summary ribbon across the top of the portal. Here you see a quick view of all of your platform elements along with highlighted numbers showing current status information.

3. Switch between **Cloud, Tenant, and Application Infrastructure**, as needed.
4. For any element displaying an error message or number, click on the error to see a popup displaying additional information about the problem.
5. Remediate the issue as instructed.

Note: You will need to be signed into Cisco IAC as the right role with the right permissions to make the necessary changes. See [Handling Infrastructure Errors, page 144](#) for more information on handling the errors you find here.

6. Click **Submit Order.**
7. Repeat as necessary for as many platform element types as you need to adjust.

8. Close this portal when you are finished.

Managing Intervals

For each platform element, use that element's Manage Intervals button to open the Update System Health Check Intervals form. To adjust *all* types at once to the same interval, use the Manage Intervals button at the top right of the screen.

1. Choose **Operations > System Health**.
2. On the System Health Status page, choose Check Intervals.

The Update System Health Check Intervals screen displays.

3. Choose a new interval as needed.
4. Click **Submit Order**.



Managing Resources Using Discovery

Discovering Network Devices

Network discovery in Cisco Intelligent Automation for Cloud 4.2 consists of discovering the network devices and links that you want Cisco IAC to go out, look for and return information on, and then registering the devices you want to use.

Running Discovery

1. Choose **Setup > Manage Infrastructure**.
2. From the menu that appears next along the left of the screen, choose **Network Elements**.
3. From the icons that display in the Network Elements drop-down list, choose **Network Devices**:
4. Click **Discover Network Devices** just below the Network Devices label towards the top of the screen.

The CloudSync Infrastructure Discovery screen displays. Note that Network Devices is already chosen in the Discovery Type drop-down list.

5. Enter an IP address in the Seed Device field for any device inside your POD.

Note: Cisco uses Cisco Device Protocol (CDP) and Link Layer Discovery Protocol (LLDP) for discovery. ELM (Enhanced Local Management Interface) is used for discovery in Frame Relay, and ILMI (Interim Local Management Interface) in ATM networks.

6. Next, enter information for either Simple Network Management Protocol for version 2 or version 3, depending on how you have your devices configured.
 - For SNMP v2, enter one or more community strings.
 - For SNMP v3, enter a user name and password.
7. Enter Secure Shell (SSH) credentials.
 - Enter a username and password, then the password again in the **Enable Password** field.
 - Enter any additional usernames and passwords, as needed.

You can enter one or more credentials, as needed, for both SNMP versions as well as for SSH. CloudSync will determine which credentials should be used for which device.

8. Click **Submit Order**.

While the discovery is in process, you will see a screen letting you know that the order has been submitted. Close this screen (using the X in the upper right).

9. To see the new list of discovered network devices, click the Refresh icon (at the upper right corner of the table), or refresh the entire page.

Discovering OpenStack Resources

If you have set up OpenStack correctly, after requisition is complete you will be able to see several OpenStack resources discovered in **Setup > Manage Infrastructure** tab.

Note: To avoid having Cloud Resources skipped during discovery, be sure to discover OpenStack Projects *before* syncing any other OpenStack Cloud Resources.

The following cloud resources are discovered for OpenStack by Cisco IAC 4.2:

- **Flavors:** The types of sizes of VMs.
Note: Cisco IAC refers to OpenStack “instances” as “VMs”.
- **Floating IP Pools:** Floating IP Pools are provisioned in Neutron during the creation of the external subnet. These are discovered and registered by Cisco IAC so that system knows about, tracks, and assigns FIPs properly.
- **Images:** These are templates that are used for VM creation.
- **Keypairs:** SSH keys for accessing VMs.
- **Networks:** Details about networks and subnets available for VMs.
- **Projects:** When a new VDC is created in Cisco IAC, this corresponds to a new Project in OpenStack.
- **Security Group:** Security policies and groups.
- **Volumes:** Detachable block storage devices, similar to USB hard drives, that can be attached to one instance at a time.

Note: Discovered OpenStack resources (such as Flavors, Floating IP Pools, Images, Volumes, and so on) should be registered in Cisco IAC the same as any other platform resources. After you have discovered OpenStack cloud resources, you then need to register a compute POD in Cisco Intelligent Automation for Cloud. For instructions on how to do so, see [Creating One or More Network PODs, page 127](#)

Registering an OpenStack Resource

After OpenStack Resources have been discovered by Cisco IAC 4.2, you can register the network resource, for example, in same way as any other discovered resources can be registered.

Note: Networks which are discovered and registered need to be created as 'Shared' networks in OpenStack. This allows them to be used in Provisioning VDCs using existing networks, as well as for Add Network to VDC.

Note: Registration is not currently supported for Security Groups in OpenStack.

1. Click the **gear** icon  next to the resource you want to register.
2. Choose **Register OpenStack Network**.
3. Complete the **Register OpenStack Network** form.
4. Enter the **Friendly Name** and (*optional*) a **Description**.
5. Choose whether this is an **External Network**.

Note: Internal networks should be selected for use as tenant networks. These must be created ahead of time in OpenStack via the API or from the Dashboard in order to discover and then register them.

6. Click **Submit**.

Managing Resources

This section describes how to use My Servers, System Resources, and CloudSync to view specifications and status, and discover new virtual and physical servers, blades, blade chassis, and data centers.

Viewing System Resource Capacity

On the System Resources portal, view the following information for your infrastructure resources:

- Capacity statistics for virtual clusters and virtual data centers
- Proportions of blades in the virtual, physical, and maintenance pools

1. Choose **Service Portal > Operations > System Resource Capacity**.

The System Resources portal displays following information

Resource	Description
Virtual Cluster Capacity	<p>Indicates CPU and memory resource capacity and allocation for each vCenter cluster.</p> <ul style="list-style-type: none"> ■ Cluster Name ■ CPU Reserved (MHz) ■ CPU Limit (MHz) ■ Memory Reserved (GB) ■ Memory Limit (GB) ■ Last Collected
Data center	Bar graphs illustrating the CPU and memory resource capacity and allocation of all resources in the vCenter data center.

2. Close the window when you are done viewing.

Managing Cloud Infrastructure Discovery

The CloudSync Infrastructure Discovery service provides Cloud Provider Technical Administrators a means for monitoring platform elements. The CloudSync service can be used to discover existing and new instances of platform elements.

When objects are first discovered, most are placed into Discovered state, while others are auto-Registered (data centers, clusters, hosts, resource pool, port groups, and UCS VLANs). All may be transitioned into service (Registered), rejected (Ignored), or set aside for future use (Maintenance).

You can define how the object will be presented to end users for consumption by providing metadata such as friendly names, descriptions, and some object-specific elements.

Take one of the following actions on an object:

- Register the object so that it is available for use in the cloud system.
- Put the object on “hold” by placing it into maintenance mode; it is not available for use until it is registered.
- Ignore the object if you do not intend it to be used.

These actions place the object into one of three states: Registered, Maintenance, or Ignored. These states may be changed at a later time. After an object has been registered, an edit action can be performed to change the display name and the description. After an object has been put in maintenance mode, it can be re-registered using the Activate action.

The Discovery portal is located on the Manage Cloud Infrastructure tab in the Service Portal module. The total number of instances of each object, new and existing, appears above the object icon; the number of new instances, if any, appears in red.

Discovering Objects in the Cloud Infrastructure

On the CloudSync Infrastructure Discovery portal, you have the following options for performing discoveries:

- Discover all instances of an object (for example, OS Templates)
- Discover all new and existing instances in a platform element type, that is, VMware vCenter, or Cisco UCS Manager.
- Discover all new and existing instances of all objects.

1. On the CloudSync Infrastructure Discovery portal, click the icon for the object.

A Discover link for the object (for example, **Discover OS Templates**) appears in the upper right corner beside **Discover All**.

2. Click the Discover link to open the Discover Infrastructure form.
3. Click **Submit Order**.

To discover all instances of a platform element type:

1. Click inside the gray frame for the platform element.

A Discover link for the group (for example, **Discover vCenter Cloud Resources**) appears in the upper right corner beside **Discover All**.

2. Click the Discover link to open the Discover Infrastructure form.
3. Click **Submit Order**.

To discover all new instances of all objects:

1. Click **Discover All** in the upper right corner of the portal to open the Discover Infrastructure form.
2. Click **Submit Order**.

Viewing Discovered Objects in the Infrastructure

View instances of all objects that were added to the system or detected during the last discovery (if any).

To view all instances of an object, click the icon of the object—for example, Clusters. The “Take Action” grid, listing all of the clusters, and three action buttons (Register, Maintenance, Ignore) appear. Those buttons that appear in color are active, indicating that their respective services are available; those in gray are inactive, indicating that their respective services are not available. To customize the columns that display in the grid, see [Customizing Table Views, page 6](#).

Note: The statuses that appear in the grid were detected in the previous discovery (if any) and are not up-to-date. To obtain current statuses, you must perform discoveries.

An object instance exists in one of the following five statuses:

- Discovered—The object was detected in the previous discovery, but no action has been taken upon it yet.

- Registered—The object has already been registered, but still needs to be processed to add user-defined fields, such as a friendly name or description. If the object was discovered and automatically set by the system to Registered state, no action is required.
- Maintenance—The object is in maintenance mode.
- Ignored—The object was rejected for use.
- Not Found—The object, which was previously discovered, was not detected in the latest discovery, for whatever reason.

Table 1 Allowed Transitions

State Name	To:	From:
Discovered	Registered, Ignored, Not Found	Not Found (only when re-discovered)
Registered	Maintenance, Not Found	Discovered, Ignored, Maintenance
Ignored	Registered, Not Found	Discovered, Registered, Maintenance
Maintenance	Registered, Ignored, Not Found	Registered
Not Found	Discovered (only when re-discovered)	Discovered, Registered, Ignored, Maintenance

Managing Authorization and Review Escalation

Only a Cloud Provider Technical Administrator has the authority to set up and modify authorizations. Use the instructions in this section to manage authorization and review escalation. An escalation is a sequence of tasks requiring action from an assigned person. The tasks are listed in Service Manager for the person to view and take action. An authorization task requires the assigned authorizer to reject or approve a service request. Authorization sequences are configurable for:

- Finance
- Departments
- Service Groups

A review task requires an assigned reviewer to sign off on a step in the delivery process. Review sequences are configurable for:

- Departments
- Service Groups

Enabling an Authorization or Review

1. Log out and log back in to get the portal picker.
2. Choose **Administration** from the module drop-down list and then click Set Up Authorization Process.
3. Click the **Edit** button next to Service Group Authorization.
4. Choose **Enabled** from the Status drop-down list.
5. Repeat steps 2 and 3 if you need to enable any other Authorizations.

Setting Up Escalation Sequences

An escalation sequence is a series of notifications triggered when a task remains incomplete within specified time limits. When a task has not been completed within the specified time, the cloud system sends an email notification to the assigned person, supervisor, and/or customer for resolution.

If the task remains incomplete after the first notification, the process is repeated for the next tier.

- For authorizations, you can specify different notification recipients for each tier in the escalation.
- For reviews, all identified recipients receive notifications for each tier. You can configure one or more tiers.
 1. Follow the steps outlined in [Enabling an Authorization or Review, page 29](#).
 2. Click **Edit** beside an authorization group in the list.
 3. In the Escalations panel, click **Add**, then provide the following information:

Table v-2

Field Name	Action
After (hours)	Enter the number of hours to elapse between escalations. For example, if this value is 8, then a notification will be sent every 8 hours until the task is resolved. Note: This value does not represent the number of hours after the due date that the first tier in the escalation is executed.
First Recipient Second Recipient Third Recipient	Enter up to three valid email addresses, separated by commas, of the persons who will receive notifications during escalation. You can also use namespace variables. For information on using namespaces, see the Cisco Service Portal Namespace Users Guide . You can configure as many tiers as needed. To add more tiers, click Add , and repeat this step for adding recipients and templates.
Email notification template	For each recipient, choose an email template to use for the notification from the drop-down list. To modify an email notification template, see Modifying Email Notification Templates, page 86 .



User Roles and Capabilities

Cisco Intelligent Automation for Cloud 4.2 (Cisco IAC) is a self-service provisioning and orchestration software solution for cloud computing and data center automation. Cisco IAC users access services and tasks using Prime Service Catalog, a browser-based interface that provides links to services and status, such as ordering servers, viewing requisitions, monitoring system resources. Cisco IAC 4.1 features seven pre-defined user roles that determine what individuals can access and perform. There are several roles aligned with each business area, listed below.

- **Cloud Provider Roles:** The group which is hosting the cloud. This may be an Enterprise IT department, or a Service Provider.
 - **Cloud Provider Technical Administrator (CPTA).** Manages cloud resources & services via the service catalog. Has access to internal network and systems (underlying cloud infrastructure). Onboards and offboards tenants.
 - **Cloud Provider Business Administrator (CPBA).** This role is associated with processing financial approvals for money being spent, managing the money and quotas associated with capacity management.
- **Tenant Roles:** A tenant represents a customer, a unique billable entity.
 - **Tenant Technical Administrator (TTA).** The catalog of services available to each tenant organization is determined by the set of elections made by a tenant administrator.
 - **Tenant Business Administrator (TBA).** Financial approval for money being spent. Can create organizations and assign Organization Technical Administrators to Organizations.
- **Organization: Each tenant has one or more organizations. An organization contains its own catalog.**
 - **Organization Technical Administrator (OTA).** Manages Server Owners, resources, and services. Orders VDCs, firewall, and load-balancing services for VDC zones and networks.
 - **Virtual Server Owner (VSO).** A consumer of the services. Orders virtual machines, firewall, and load-balancing services for their virtual servers.
 - **Virtual Physical and Server Owner (VPSO).** A consumer of the services. Orders physical and virtual machines, firewall, and load-balancing services for their servers.
- **Other:**
 - **Solutions Team (ST).** Has permissions to perform specific tasks in Service Groups, Active Form Components (AFCs), and Dictionaries.
 - **Form Extender (FE).** Has permissions to perform specific tasks in Service Groups, Active Form Components (AFCs), and Dictionaries.
 - **Stack Designer (SD).** Has permissions to create new stacks, rearrange stacks, and name stacks.

Note: A “Tenant” Technical Administrator role has capabilities and permissions within the system greater than (a superset of) those given to their Business Administrator counterpart. For example, business roles do not have authority to order Virtual Machines. Additionally, the system-defined “Anyone” role includes all of the Prime Service Catalog roles within an organization. This role is a selectable option for certain user properties that identify individuals who can order on behalf of the user and read or change the user’s record.

User Roles

Cloud Provider Technical Administrator

The Cloud Provider Technical Administrator (CPTA) manages both the underlying infrastructure as well as the Cisco IAC cloud management software. As employees of the service provider, Cloud Provider Technical Administrators are responsible for purchasing, installing, and configuring the Cisco IAC solution, then inviting customers to be customers of the Cloud solution. Cloud Provider Technical Administrators have access to the following modules:

- Service Portal
 - Access and perform tasks from all portals and portlets.
- Service Manager
 - Categorize and process service request approvals and perform other manual tasks that arise during service delivery.
 - Manage standards for service items, such as lease terms, network types, operating system types, platform element types and options, and so on.
- Service Item Manager
 - Create or modify ordering standards such as available server sizes and managed lease term limits, among other examples (e.g., managing the VDC Topology offerings).
 - Manage all Service Item tables.
- Administration
 - Link to and utilize data from your enterprise directory and other sources of user data.
 - Customize your Prime Service Catalog environment with colors and branding, and turn on or off various site-wide settings, such as custom style sheets and directory integration.
 - Modify standard lists of values used across the site and in related reports.

Cloud Provider Business Administrator

The Cloud Provider Business Administrator (CPBA) is in charge with overseeing and administrating a public or private cloud as a revenue generating business. This covers:

- Determining the mix of services that the public or private cloud is offering in the market.
- Determining the pricing of services and service options.
- Handling the business interaction with individual tenants.

Note: When operating a private cloud, even one including tenants, IT does run a business. Therefore, the role of the Cloud Provider Business Administrator (CPBA) may be reduced in some organizations to exclude the second bullet item, above, “Determining the pricing of services and service options.” In addition, while CPBAs have the ability to control who gets to order what (service offerings), they themselves cannot actually place an order.

Tenant Technical Administrator

The Tenant Technical Administrator (TTA) is an employee of the organization who manages tenants from a technical standpoint. In a self-managed tenant, a Tenant Technical Administrator is the administrative authority within the tenant on all technical matters related to using the cloud system, and is the tenant's technical representative to the cloud provider.

User Roles

TTAs do the following:

- Manage the tenant's user accounts and organizational structure.
- Manage tenant's Virtual Data Centers and related elements.
- Manage tenant-wide services offered to all their organizations.

In this regard, the TTA assumes some of the responsibility of a CPTA in a single tenant (no-tenant) private cloud. In provider-managed tenants, the tenant hires the cloud provider to perform all administrative duties. As a result, there may not be a tenant user that acts as a TTA. A provider user will be appointed to perform the above duties and order on behalf of the tenant.

Each tenant has at least one Tenant Technical Administrator, whose account is typically created when the tenant is first created. The Tenant Technical Administrator can create Organizational Technical Administrators and Cloud End-Users. The Tenant Technical Administrator role may be assigned by a CPTA or another TTA. A Tenant Technical Administrators role would have the rights over all objects owned by organizations for the tenant.

Tenant Business Administrator

The Tenant Business Administrator (TBA) is an employee of the organization who manages tenants from a business standpoint. In a multi-tenant cloud, the Tenant Business Administrator is the commercial and business authority within the tenant and represent these concerns to the cloud provider. These responsibilities include:

- Negotiate pricing, service options, service levels and other service terms with the cloud provider.
- Approve high cost service orders by tenant users.
- Analyze cloud costs to the tenant, over time, by service, by organization, in order to control costs and ensure the best return on investment.

In a provider-managed tenant, since there may not be a tenant user that is a technical administrator, the TBA serves as a the only tenant representative.

Note: In private clouds with multiple tenants, there may not be a TBA user; and if there is, their role may be reduced to only perform the last two bullet items above.

Organization Technical Administrator

An Organization Technical Administrators (OTA) is an employee of the organization with some administrative access and control over their organization's environment. The Organization Technical Administrators manage an organization's user accounts, virtual data centers, and organization-specific service catalogs in Prime Service Catalog. They also assign users to Server Owner roles within the organization. The Organization Technical Provider has access to the following modules:

- Service Portal – Access the following pages to order Prime Service Catalog services:
 - My Servers – View a list of all of the servers you own or manage, and perform actions such as powering up or down, taking a snapshot, or decommissioning.
 - User Management – Add, modify, and remove OTA, VPSO, and VSO users.
 - Order Cloud Services–Commission a virtual machine or physical server or VDC, manage load-balancers, or manage network zone security within VDCs.
 - Create users and update user profile information.
 - View own and Organization's constituent users' Run Rate—the set of recurring charges incurred for cloud services they or their users have purchased.

User Roles

- View details and manage network topology and capacity of VDCs to which the OTA has access. May grant other organizations access to their VDCs.
- View their prior orders and current order status (for themselves and users within their organization).

Virtual and Physical Server Owner

The Virtual and Physical Server Owner (VPSO) is an employee of the organization who orders and provisions both virtual and physical servers. The Virtual and Physical Server Owner has access to the following portal pages in the Service Portal module:

- My Servers—View a list of all of the servers you own or manage, and perform actions such as powering up or down, taking a snapshot, or decommissioning.
- Order Cloud Services—Commission or decommission a virtual or physical server.
- View Run Rate—View the set of recurring charges incurred for the cloud services purchased.
- View Details—View details, topology, and capacity of VDCs to which the user has access.
- View Orders—View prior orders and current order status.

Virtual Server Owner

The Virtual Server Owner (VSO) is an employee of the organization who orders and provisions virtual machines. The Virtual Server Owner has access to the following portals in the Service Portal module:

- My Servers—View a list of all of the servers you own or manage, and perform actions such as powering up or down, taking a snapshot, or decommissioning.
- Order Cloud Services—Commission or decommission a virtual server, or firewall and load-balancing services.
- View Run Rate—View the set of recurring charges incurred for the cloud services purchased.
- View Details—View details, topology, and capacity of VDCs to which the user has access.
- View Orders—View prior orders and current order status.
- My Applications—Manage applications.

Solutions Team

The Solutions Team (ST) member has permissions to perform the tasks in the following categories:

- Service Groups
 - Assign Rights and View Services in service groups that contain Cisco content solutions.
 - Design services, assign rights, and view services in service groups that contain Cisco content solution extensions.
 - View all aspects of the service definition.
- Active Form Components (AFCs)
 - “View Form” permission in AFC groups that contain Cisco content solutions.
 - “View Forms” and “Design Forms” permissions in AFC groups that contain Cisco content solution extensions.
- Dictionaries

Capabilities by User Role

- Read permission in dictionary groups that contain Cisco content solutions.
- Read/write permissions in dictionary groups that contain Cisco content solution extensions.

Form Extender

The Form Extender (FE) has permissions to perform the tasks in the following categories:

- Service Groups
 - Design Services, Assign Rights and View Services in service groups that contain Cisco content solutions, but can only see the **Form** tab.
 - Design Services, Assign Rights and View Services in service groups that contain Cisco content solution extensions, but can only see the **Form** tab.
- Active Form Components (AFCs)
 - “View Form” permission in AFC groups that contain Cisco content solutions.
 - “View Forms” and “Design Forms” permissions in AFC groups that contain Cisco content solution extensions.
- Dictionaries
 - Read permission in dictionary groups that contain Cisco content solutions.
 - Read/write permissions in dictionary groups that contain Cisco content solution extensions.

Capabilities by User Role

The table below shows the capabilities by user role.

Table 1 Capabilities by User Role

Category	Service	CPTA	CPBA	TTA	TBA	OTA	VPSO / VSO	ST	FE
Agents	Configure HTTPS agents	●	○	○	○	○	○	○	○
	Configure REX agents	●	○	○	○	○	○	○	○
Cisco UCS Blades	Register a Cisco UCS blade	●	○	○	○	○	○	○	○
	Manage blade pools	●	○	○	○	○	○	○	○
	Remove a Cisco UCS blade	●	○	○	○	○	○	○	○

Capabilities by User Role

Table 1 Capabilities by User Role (continued)

Category	Service	CPTA	CPBA	TTA	TBA	OTA	VPSO / VSO	ST	FE
Metrics	Assign cluster metric service item data	●	○	○	○	○	○	○	○
	Assign data center metric service item data	●	○	○	○	○	○	○	○
	Assign datastore metric service item data	●	○	○	○	○	○	○	○
	Assign IP Address service item data	●	○	○	○	○	●	○	○
	Assign network metric service item data	●	○	○	○	○	○	○	○
	Assign resource pool metric SI data	●	○	○	○	○	○	○	○
	Assign Cisco UCS metric service item data	●	○	○	○	○	○	○	○
	Refresh metrics	●	○	○	○	○	○	○	○
Networks	Add or remove a network	●	○	○	○	○	○	○	○
Ordering Servers	Create Container from Template and Install OS	●	○	●	○	●	●	○	○
	Order a virtual machine and install an operating system	●	○	○	○	●	●	○	○
	Order a virtual machine from template	●	○	●	○	●	●	○	○
	Decommission a virtual machine	●	○	●	○	●	●	○	○
	Order a physical server	●	●	●	○	●	●	○	○
	Decommission a physical server	●	●	●	○	●	●	○	○
	Define a managed lease instance for a new server	●	●	●	●	○	●	○	○
	Extend a managed lease instance on a server	●	●	●	●	●	●	○	○
Organizations	View organization details	●	●	●	●	●	○	○	○
	Create, modify, remove an organization	○	○	●	●	●	○	○	○
	Add or remove an organization network	●	●	●	●	○	○	○	○
	Add or modify the Cloud Administration organization	●	●	●	●	○	○	○	○
Virtual Data Centers	Create virtual data center	●	●	●	○	●	○	○	○
	Decommission virtual data center	●	●	●	○	●	○	○	○
	Modify VDC size	●	●	●	○	●	○	○	○
	Add network to VDC	●	●	●	○	●	○	○	○
	Remove network from VDC	●	●	●	○	●	○	○	○

Capabilities by User Role

Table 1 Capabilities by User Role (continued)

Category	Service	CPTA	CPBA	TTA	TBA	OTA	VPSO / VSO	ST	FE
Server Administration	Add or remove a user as a Server Owner	●	●	●	●	●	○	○	○
	Assign or remove a Cloud Provider Technical Administrator	●	●	○	○	○	○	○	○
	Assign or remove Organization Technical Administrator	●	●	○	○	●	○	○	○
Users and Cisco IAC Roles	Modify user properties	●	●	○	○	●	○	○	○
	View Cloud Provider Technical Administrator role settings	●	●	●	●	○	○	○	○
	View Organization Technical Administrator role settings	●	○	●	●	●	○	○	○
	View Virtual Server Owner role settings	●	○	●	●	○	●	○	○
	View Virtual Server Owner role settings	●	○	●	●	○	○	○	○
	View Form Extender Role settings	●	○	●	●	○	○	○	●
	View Solutions Team role settings	●	○	●	●	○	○	●	○
Server Operations	Modify Server Configuration	●	●	●	○	●	●	○	○
	Power-up, power-down, power-cycle a Virtual Machine	●	●	●	○	●	●	○	○
	Take, revert-to, or remove a server snapshot	●	●	●	○	●	●	○	○
	Add volumes in OpenStack	●	○	●	○	●	●	○	○
	Clone VM to vApp	●	○	●	○	●	●	○	○
System Setup and Management	Connect or update the cloud infrastructure	●	○	○	○	○	○	○	○
	Configure the email notification templates	●	○	○	●	○	○	○	○
	Set provisioning Settings	●	○	○	○	○	○	○	○
	Set up or update the shared server zone	●	○	○	○	○	○	○	○
	Validate platform elements	●	○	○	○	○	○	○	○
Server Templates	Register or Update Service Profile Template	●	○	○	○	○	○	○	○
	Register VM Template	●	○	○	○	○	○	○	○
	Register Operating System Template	●	○	○	○	○	○	○	○

Support for Multiple Cloud Platforms

The table below details the support for multi-cloud platforms.

Table 2 Support for Multiple Cloud Platforms

	VMware vCenter Server	VMware vCloud Director	OpenStack Cloud Manager	Cisco UCS Manager	Cisco UCS Director	Amazon EC2
Add Cisco APIC Network Policy, OpenStack Cloud Manager <i>new for 4.2</i>	●	●	●	○	○	○
Add Manage Volumes, OpenStack Cloud Manager <i>new for 4.2</i>	●	●	●	○	○	○
Add a Network to VDC	●	●	●	○	○	○
Add Member to Server Group	●	○	○	○	○	○
Add Member to Service Group	●	○	○	○	○	○
Add to Server Group	●	●	○	N/A	○	○
Allocate Floating IP Address	●	●	○	●	○	○
Clone VM to Template	○	●	○	N/A	○	○
Clone VM to vApp	●	●	○	N/A	○	○
Convert VM to Template	●	●	○	N/A	○	○
Create Container from Template	○	●	○	○	○	○
Create Physical Firewall Rule	●	●	○	●	○	○
Create Server Group	●	○	○	○	○	○
Create VM Firewall Rule	●	●	○	N/A	○	○
Create VM Firewall Rule	○	○	○	N/A	○	○
Decommission VDC	●	●	●	○	○	○
Decommission Virtual Machine	●	●	●	N/A	●	●
Delete LB Service Group	●	○	○	○	○	○
Delete Server Firewall Rule	●	●	○	●	○	○
Delete Server Group	●	○	○	○	○	○
Delete Service Group	●	○	○	○	○	○
Delete Snapshot	●	●	●	N/A	●	●
Manage Access to VDC	●	●	●	○	○	○
Manage Load Balancer	●	●	○	N/A	○	○
Manage Service Group Membership	●	○	○	○	○	○
Modify Configuration	●	●	●	N/A	○	○
Modify Network Properties	○	○	○	○	○	○
Modify Server Ownership	●	●	●	●	●	●
Modify VDC Size	●	●	●	○	○	○
Order a Virtual Machine from Template	●	●	●	●	●	●
Power Cycle Virtual Machine	●	●	●	N/A	●	●
Power Down Virtual Machine	●	●	●	N/A	●	●
Power Up Virtual Machine	●	●	●	N/A	●	●
Remove from Server Group	●	●	○	N/A	○	○

Table 2 Support for Multiple Cloud Platforms (continued)

	VMware vCenter Server	VMware vCloud Director	OpenStack Cloud Manager	Cisco UCS Manager	Cisco UCS Director	Amazon EC2
Remove Member from Server Group	●	○	○	○	○	○
Remove Network from VDC	●	●	●	○	○	○
Remove Physical Firewall Rule	●	●	○	●	○	○
Remove VM Firewall Rule	○	○	○	N/A	○	○
Revert to Snapshot	●	●	●	N/A	●	●
Take Snapshot	●	●	●	N/A	●	●
Update LB Service Group	●	○	○	○	○	○
View Snapshots	●	●	●	N/A	●	●



Setting Up the Infrastructure

This section describes:

- Connecting Cloud Platform Elements, which include:
 - Amazon EC2
 - AMQP Server
 - Chef
 - Cisco Application Policy Infrastructure Controller (Cisco APIC) *new for 4.2*
 - Cisco IAC Management Appliance
 - Cisco Prime Network Registrar IPAM
 - Cisco Prime Network Services Controller (PNSC)
 - Cisco Prime Performance Manager
 - Cisco Process Orchestrator
 - Cisco Unified Computing System (UCS) Director
 - Cisco Unified Computing System (UCS) Manager
 - OpenStack Cloud Manager
 - Puppet
 - VMware vCenter Server
 - VMware vCloud Director
 - Setting up REX

Note: As you define each platform element for the platforms that have discovery, the discovery process automatically begins and runs in the background. If there is a discovery error for the platform element, you will receive an e-mail notification. Not all platforms have discovery.

Note: Notifications of discovery errors will be set to the notifications e-mail address for the Cloud Service Approval Administration queue. If you have not done so, return to [Assigning Mail Addresses for Queue Notifications, page 67](#), for instructions before you proceed with the tasks in this section. Note that not all platforms have discovery.

This section also covers:

- Setting Provisioning Settings
- Setting System-Wide Service Options
- Remediating Platform Element Errors
- Creating One or More PODs

- Registering a Datastore
- Setting Up REX and nsAPI User Accounts
- Setting DB, HTTP, NSAPI Agents Configuration
- Setting Up a Community VDC
- Creating an Organization
- Creating a New User to Add as an Organization Technical Administrator (OTA)
- Adding a Server Owner
- Assigning Mail Addresses for Queue Notifications

Connecting the Cloud Platform Elements

You must first define the connection information for the platform elements that will be used in Cisco Intelligent Automation for Cloud 4.2. This section describes how to define the connections for the following platform elements (all of which are associated with a Compute “Point of Delivery” or POD).

Defining the Amazon EC2 Platform Element

You must be logged in as the Cloud Provider Technical Administrator to perform this task. Complete the following steps to define the connection information for the Amazon EC2 platform element that will be used in Cisco Intelligent Automation for Cloud 4.2. You may establish any number of EC2 connections.

1. Launch Cisco IAC and log in as a Cloud Provider Technical Administrator.
2. Choose **Setup > System Settings > Connections** tab.
3. On the Connections tab, click **Connect Cloud Infrastructure** to open the form.
4. On the Connect Cloud Infrastructure form, choose **Amazon EC2** from the Platform Element Type drop-down list.
5. Specify the following connection information for the Amazon EC2 connection:
 - Enter the **Connection Name**. This is the “friendly name” for the Amazon EC2 connection.
 - Enter the **Region Host Name**. This is the host name or IP address for the Amazon EC2 region.
 - Enter a **Description** (optional).
 - Click the **True** or **False** radio button to indicate whether certificate error messages should be ignored. **True** is chosen by default.
 - Enter an **Availability Zone** (optional) for the region identified above.
 - Enter an Amazon **Access Key** for authentication with AWS.
 - Enter the Amazon EC2 **Secret Key** for the access key above. The reenter the secret key.

Caution: Be sure to set the “File Share Path” global variable so that Amazon EC2 virtual machines can be successfully ordered when using key pairs.

6. Click **Submit Order**.

Defining the AMQP Server Platform Element

You must be logged in as the Cloud Provider Technical Administrator to perform this task. Complete the following steps to define the connection information for the AMQP server platform element that will be used in Cisco Intelligent Automation for Cloud 4.2. You can define a connection between one AMQP and one Cisco Prime Performance Manager only.

1. Launch Cisco IAC 4.2 and log in as a Cloud Provider Technical Administrator.
2. Choose **Setup > System Settings > Connections** tab.
3. On the Connections tab, click **Connect Cloud Infrastructure** to open the form.
4. On the Connect Cloud Infrastructure form, choose **AMQP Server** platform element from the Platform Element Type drop-down list.
5. Specify the following connection information for the AMQP Server platform element:
 - Enter the **Connection Name**. This is the “friendly name” for the AMQP Server element connection.
 - Enter the **Host Name**. This is the host name or IP address for the AMQP Server element.
 - Enter the **Port**. This is the TCP/IP port used to connect to the AMQP server.
 - Enter a **Description** (optional).
 - Enter the virtual host name of the AMQP Server.
 - Click the **True** or **False** radio button to indicate whether secure connection protocol is used to connect to the server. **False** is chosen by default.
 - Click the **True** or **False** radio button to indicate whether certificate error messages should be ignored. **False** is chosen by default.
 - Enter a **User Name**. This is the account name to use when connecting for the platform element
 - Enter the **Password** used to connect to the AMQP Server then re-enter the **Password** to confirm it.
6. Click **Submit Order**.

Defining the Chef Platform Element

You must be logged in as the Cloud Provider Technical Administrator to perform this task. Complete the following steps to define the connection information for the Chef Platform Element that will be used in Cisco Intelligent Automation for Cloud 4.2. You may register/connect to any number of Chef servers.

Note: Cisco IAC uses the Chef “knife” tool, which should be installed and working correctly on Chef server.

1. Launch Cisco IAC 4.2 and log in as a Cloud Provider Technical Administrator.
2. Choose **Setup > System Settings > Connections** tab.
3. On the Connections tab, click **Connect Cloud Infrastructure** to open the form.
4. On the Connect Cloud Infrastructure form, choose **Chef** from the Platform Element Type drop-down list.
5. Specify the following connection information for the Chef platform element:
 - Enter the **Connection Name**. This is the “friendly name” for the Chef platform element connection.
 - Optional. Enter information that describes the Chef platform element.

- Enter the **Host Name**. This is the host name or IP address for the Chef platform element server.
 - Enter the **SSH Login** and **SSH Password** assigned to the account used to connect to the Chef platform element server.
 - Re-enter the SSH Password to confirm it.
 - Enter the **Private Key**. (This is optional. Not all deployments require this.)
6. Check the **Show Additional Options** check box (optional). Here you can add additional information such as:
- **Installer Package Base URL**. This is the Base URL for downloading the Chef installer package. Default location is Chef repository. This can also be a local HTTP resource where installer packages are stored.
Note: If left blank, it will use the online public Chef repository.
 - **Alternate Module Path**. By default, discovery uses the modulepath as defined in chef.conf. You can point discovery to an alternate path such as a GIT working copy. In defining an alternate path, you can use `$environment` to dynamically insert the environment in the path.
 - **Hiera Node Classification Path**
Note: New nodes are classified using Hiera Yaml files, and, by default, are saved to the Chef location specified by the first folder specified in the module path. These files can be stored in an alternate location, perhaps separate from your modules. In defining the hiera path, you can use `$environment` to dynamically insert the environment in the path. Remember, this location must match what is defined in your hiera.yaml file in the Chef's configuration directory.
 - Set up **Linux Proxy**.
 - Set up **Linux Proxy Bypass**.
 - Enter the **Linux Bootstrap User** and **Linux Bootstrap Password**.
 - Set up **Windows Proxy**.
 - Set up **Windows Proxy Bypass**.
 - Enter the **Windows Bootstrap User** and **Windows Bootstrap Password**.
7. Click **Submit Order**.

Defining the Cisco Application Policy Infrastructure Controller (Cisco APIC) Platform Element

Note: For more information on Cisco APIC and OpenStack, refer to detailed APIC documentation located here: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/api/openstack/b_Cisco_APIC_OpenStack_Driver_Install_Guide.html.

You must be logged in as the Cloud Provider Technical Administrator (CPTA) to perform this task. Complete the following steps to define the connection information for Cisco Application Policy Infrastructure Controller (Cisco APIC) that will be used in Cisco Intelligent Automation for Cloud 4.2. Only one Cisco APIC platform element may be registered.

1. Launch Cisco Intelligent Automation for Cloud 4.2 and log in as a Cloud Provider Technical Administrator.
2. Choose **Setup > System Settings > Connections** tab.
3. On the Connections tab, click **Connect Cloud Infrastructure** to open the form.
4. On the Connect Cloud Infrastructure form, choose **Cisco APIC** from the Platform Element Type drop-down list.
5. Specify the following connection information for the APIC connection:

Connecting the Cloud Platform Elements

- a. Enter the **Connection Name**. This is the “friendly name” for the APIC connection.
 - b. Enter the **Host Name**. This is the host name or IP address for APIC.
 - c. *Optional*. Enter information that describes this Cisco APIC connection.
 - d. The **True** or **False** radio button to indicates whether secure connection protocol is used to connect to the server. *True* is chosen by default. Because Cisco APIC requires a Secure Connection for API communications, this should be left at **True**.
 - e. Click the **True** or **False** radio button to indicate whether certificate error messages should be ignored. *True* is chosen by default. For API communications, this should be left at **True**.
 - f. Enter the **User Name** to use when connecting to Cisco APIC.
 - g. Enter the **Password** assigned to the account used to connect to APIC.
 - h. Re-enter the password to confirm it.
6. Click **Submit Order**.

About Cisco APIC

Cisco APIC supports the deployment, management, and monitoring of any application anywhere, with a unified operations model for the physical and virtual components of the infrastructure. APIC programmatically automates network provisioning and control that is based on the application requirements and policies. Cisco IAC 4.2 speaks to APIC directly with HTTP API requests, similar to how Cisco IAC communicates with OpenStack. We do this to create network policy in ACI (Cisco Application Centric Infrastructure, a distributed, scalable, multi-tenant infrastructure) where our networks act as endpoints. For more information, see the [Cisco APIC REST API User Guide](http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/api/rest/b_APIC_RESTful_API_User_Guide/b_IFC_RESTful_API_User_Guide_chapter_01.html), especially the section, “[Overview of the APIC REST API](#)” here:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/api/rest/b_APIC_RESTful_API_User_Guide/b_IFC_RESTful_API_User_Guide_chapter_01.html

Defining the Cisco IAC Management Appliance Platform Element

You must be logged in as the Cloud Provider Technical Administrator to perform this task. Complete the following steps to define the connection information for the Cisco IAC Management Appliance platform element that will be used in Cisco Intelligent Automation for Cloud 4.2. You may connect to only one Cisco IAC Management Appliance.

1. Launch Cisco Intelligent Automation for Cloud 4.2 and log in as a Cloud Provider Technical Administrator.
2. Choose **Setup > System Settings > Connections** tab.
3. On the Connections tab, click **Connect Cloud Infrastructure** to open the form.
4. On the Connect Cloud Infrastructure form, choose **Cisco IAC Management Appliance** from the Platform Element Type drop-down list.
5. Specify the following connection information for the Cisco IAC Management Appliance platform element:
 - Enter the **Connection Name**. This is the “friendly name” for the Cisco IAC Management Appliance element connection.
 - Enter the **Host Name**. This is the host name or IP address for the Cisco IAC Management Appliance element.
 - Enter a **Description** (optional).
 - Enter the **Port**. This is the TCP/IP port used to connect to the Cisco IAC Management Appliance.

- Enter the virtual host name or IP address of the Cisco IAC Management Appliance.
- Click the **True** or **False** radio button to indicate whether secure connection protocol is used to connect to the server. **False** is chosen by default.
- Click the **True** or **False** radio button to indicate whether certificate error messages should be ignored. **False** is chosen by default.
- Enter the required **User Name** of “admin” (without the quotes). This is the account name to use when connecting for the platform element
- Enter the **Key to Access Assurance Control** key.

This must be the same password that was entered for the “Assurance Control Password” property during the installation procedure for the Cisco IAC Management Appliance.

- Enter the Administrator **Password** assigned to the account used to connect to the Cisco IAC Management Appliance.

This must be the same password that was entered for the “Application Server Password” property during the installation procedure for the Cisco IAC Management Appliance.

- Re-enter the **Password** to confirm it.

6. Click **Submit Order**.

Changing Management Appliance Configuration Parameters

Changing Cisco Process Orchestrator Parameters

To change any password or parameter related to Process Orchestrator, run the script (as explained below) with the new values you would like to set. This will update the configuration file and restart the XMP services.

Input

```
/opt/cisco/bin/configureXmpIacListener.pl -u <username> -P <password> -h <hostname> [-p <port>] -a
<basic|windows> [-d <Windows NT domain>] [-o <OVA file directory>]
```

Output

```
Writing xmp configuration file, /opt/cisco/XMP_Platform/discovery/conf/iac.properties
xmp is running (pid 17908)
Restarting the xmp service.
Stopping service: xmp ...Stopping xmp: [ OK ]
Starting service: xmp ...Starting xmp: [ OK ]
```

Changing the Assurance Control Password

1. First, ensure you have the current Assurance Control Password. To do so, follow the steps below.

- a. Retrieve the current randomly-generated value of the Assurance Control Password set for Barbican:

Input

```
cat /opt/cisco/assurancecontrol/webapp/assurancecontrol/authentication/key.txt
```

Output

```
{"username": "assurancecontrol", "password": "vPRkWiEoxg4vLRt1zEHS9uBBXKe5GJ.G", "tenant": "assurancecontrol"}
```

- b. Then use the Barbican OpenStack client with the username/password/tenant combination to query the Barbican database about the assurance secret.

– Retrieve the URI for the assurance secret:

Connecting the Cloud Platform Elements

Input

```
barbican --os-auth-url=http://localhost:5000/v2.0 --os-username assurancecontrol --os-password
"vPRkWiEoxg4vLRt1zEHS9uBBXKe5GJ.G" --os-tenant-name assurancecontrol secret list --name assurance
```

Output

```
Secret - href:
http://localhost:9311/v1/2c6f4633b24741ad9f19378bab46ca1e/secrets/cdde5c5c-e0cc-4974-92c2-c61e26ad7
055
    name: assurance
    created: 2015-03-25 15:15:20.619843+00:00
    status: ACTIVE
    content types: {'default': 'text/plain'}
    algorithm: None
    bit length: None
    mode: None
    expiration: None
```

- Use the URL to decrypt the Assurance Secret:

Input

```
barbican --os-auth-url=http://localhost:5000/v2.0 --os-username assurancecontrol --os-password
"vPRkWiEoxg4vLRt1zEHS9uBBXKe5GJ.G" --os-tenant-name assurancecontrol secret get
http://localhost:9311/v1/2c6f4633b24741ad9f19378bab46ca1e/secrets/cdde5c5c-e0cc-4974-92c2-c61e26ad7
055 --decrypt
```

Output

```
b'{"url": "http://www.cisco.com", "login": "assurance", "password": "assurance"}'
```

The current password is "assurance"

2. Change the assurance secret password:**Input**

```
curl --user assurance:currentPassword -k -H "Content-Type: application/json" -X PUT -d
'{"name": "assurance", "url": "http://www.cisco.com", "login": "assurance", "password": "newPassword"}'
https://localhost:5001/credentials/api/v1.0/updatecred
```

Output

```
{"message": null, "success": true}
```

Note: To confirm the new value is in place, repeat steps [1.a](#) and [1.b](#).

3. Login to Cisco IAC and update the CIAC Management Appliance platform element.

Note: Ensure to provide the new value of Assurance Control password.

Changing the Administrator Password for the Cisco User

1. As root, run the following command:

```
passwd cisco
```

2. Propagate the new cisco user credential to the Cisco Prime Performance Manager (PPM) secret in Barbican.

- Ensure you have the current assurance control password. (Refer to section [Changing the Assurance Control Password, page 46](#), steps [1.a](#) and [1.b](#), if needed.)

b. Update the ppm secret to reflect the Cisco user new credentials**Input**

```
curl --user assurance:currentAssurancePwd -k -H "Content-Type: application/json" -X PUT -d
'{"name": "ppm", "url": "https://<applianceIP>:4440", "login": "cisco", "password": "newCiscoUserPwd"}'
https://localhost:5001/credentials/api/v1.0/updatecred
```

Output

```
{"success": true, "message": null}
```

3. To confirm the new PPM secret is in place:**a. Get the ppm secret URL:****Input**

```
barbican --os-auth-url=http://localhost:5000/v2.0 --os-username assurancecontrol --os-password
"vPRkWiEoxg4vLRt1zEHS9uBBXKe5GJ.G" --os-tenant-name assurancecontrol secret list --name ppm
```

Output

```
Secret - href:
http://localhost:9311/v1/2c6f4633b24741ad9f19378bab46ca1e/secrets/99f8de9f-3e52-4d34-931f-a8e448ace
7d8
    name: ppm
    created: 2015-03-25 15:15:22.310778+00:00
    status: ACTIVE
    content types: {'default': 'text/plain'}
    algorithm: None
    bit length: None
    mode: None
    expiration: None
```

b. Use the URL decrypt the ppm secret**Input**

```
barbican --os-auth-url=http://localhost:5000/v2.0 --os-username assurancecontrol --os-password
"vPRkWiEoxg4vLRt1zEHS9uBBXKe5GJ.G" --os-tenant-name assurancecontrol secret get
http://localhost:9311/v1/2c6f4633b24741ad9f19378bab46ca1e/secrets/99f8de9f-3e52-4d34-931f-a8e448ace
7d8 --decrypt
```

Output

```
b'{"login": "cisco", "password": " newCiscoUserPwd", "url": "https://10.201.112.20:4440"}'
```

Changing the Application Server Administrator Password for Admin Users**1. Change the admin user password in the following files**

```
/opt/CSCOppm-unit/tomcat/conf/tomcat-users.xml
/opt/CSCOppm-gw/tomcat/conf/tomcat-users.xml
/opt/cisco/XMP_Platform/apache-tomcat-7.0.40/conf/tomcat-users.xml
```

2. Restart XMP service.**3. Restart PPM service.****4. Login to CIAC and update the Cisco IAC Management Appliance platform element.**

Note: Be sure to enter the new admin password that you just created.

Defining the Cisco Prime Network Registrar IPAM Platform Element

You must be logged in as the Cloud Provider Technical Administrator to perform this task. Complete the following steps to define the connection information for the Cisco Prime Network Registrar IPAM that will be used in Cisco Intelligent Automation for Cloud 4.2.

Note: For information about configuring Cisco IAC with IPAM, please go to <http://www.cisco.com/c/en/us/support/docs/cloud-systems-management/intelligent-automation-cloud/115946-CPNR-IPAM-00.html>.

1. Launch Cisco Intelligent Automation for Cloud 4.2 and log in as a Cloud Provider Technical Administrator.
2. Choose **Setup > System Settings > Connections** tab.
3. On the Connections tab, click **Connect Cloud Infrastructure** to open the form.
4. On the Connect Cloud Infrastructure form, choose **Cisco Prime Network Registrar IPAM** from the Platform Element Type drop-down list.
5. Specify the following connection information for Cisco Prime Network Registrar IPAM:
 - Enter the **Connection Name**. This is the “friendly name” for Cisco Prime Network Registrar IPAM connection.
 - Enter the **Host Name**. This is the host name or IP address for Cisco Prime Network Registrar IPAM.
 - Enter the Port. This is the TCP/IP port used to connect to Cisco Prime Network Registrar IPAM platform element.
 - Click the **True** or **False** radio button to indicate whether certificate error messages should be ignored. **True** is chosen by default.
 - *Optional.* Enter information that describes Cisco Prime Network Registrar IPAM.
 - Enter the **User Name** to use when connecting to Cisco Prime Network Registrar IPAM.
 - Enter the **Password** assigned to the account used to connect to Cisco Prime Network Registrar IPAM.
 - Re-enter the password to confirm it.
6. Click **Submit Order**.

Defining the Cisco Prime Network Services Controller Platform Element

You must be logged in as the Cloud Provider Technical Administrator to perform this task. Complete the following steps to define the connection information for Cisco Prime Network Services Controller (PNSC) that will be used in Cisco Intelligent Automation for Cloud 4.2. You can connect any number of PNSC platform elements.

1. Launch Cisco Intelligent Automation for Cloud 4.2 and log in as a Cloud Provider Technical Administrator.
2. Choose **Setup > System Settings > Connections** tab.
3. On the Connections tab, click **Connect Cloud Infrastructure** to open the form.
4. On the Connect Cloud Infrastructure form, choose **Cisco Prime Network Services Controller** from the Platform Element Type drop-down list.
5. Specify the following connection information for Cisco Prime Network Services Controller:
 - For the **NSC Controller**, choose whether to Connect to Existing Controller or to Provision a New Controller.

Note: When you Provision a New Controller you are prompted for two additional settings: **Domain** and **Resource Name**.

- Enter the **Connection Name**. This is the “friendly name” for Cisco PNSC.
 - Enter the **Host Name**. This is the host name or IP address for Cisco PNSC.
 - Click the **True** or **False** radio button to indicate whether secure connection protocol is used to connect to the server. *True* is chosen by default.
 - Click the **True** or **False** radio button to indicate whether certificate error messages should be ignored. *True* is chosen by default.
 - Enter the **User Name** to use when connecting to Cisco PNSC.
 - Enter the **Shared Secret** assigned to the account used to connect to Cisco PNSC.
 - Re-enter the shared secret to confirm it.
 - Enter the **Password** assigned to the account used to connect to Cisco PNSC.
 - Re-enter the password to confirm it.
6. Click **Submit Order**.

Defining the Cisco Prime Performance Manager (PPM) Platform Element

You must be logged in as the Cloud Provider Technical Administrator (CPTA) to perform this task. Complete the following steps to define the connection information for Cisco Prime Performance Manager (PPM) that will be used in Cisco Intelligent Automation for Cloud 4.2. Only one Cisco Prime Performance Manager platform element may be registered.

1. Launch Cisco Intelligent Automation for Cloud 4.2 and log in as a Cloud Provider Technical Administrator.
2. Choose **Setup > System Settings > Connections** tab.
3. On the Connections tab, click **Connect Cloud Infrastructure** to open the form.
4. On the Connect Cloud Infrastructure form, choose **Cisco Prime Performance Manager** from the Platform Element Type drop-down list.
5. Specify the following connection information for Cisco Prime Performance Manager:
 - Enter the **Connection Name**. This is the “friendly name” for the Cisco Prime Performance Manager connection.
 - Enter the **Host Name**. This is the host name or IP address for Cisco Prime Performance Manager.
 - Enter the **Port**. This is the TCP/IP port used to connect to Cisco Prime Performance Manager. The default is 4440.
 - *Optional*. Enter information that describes Cisco Prime Performance Manager.
 - Click the **True** or **False** radio button to indicate whether secure connection protocol is used to connect to the server. *True* is chosen by default.
 - Click the **True** or **False** radio button to indicate whether certificate error messages should be ignored. *True* is chosen by default.
 - Enter the **User Name** to use when connecting to Cisco Prime Performance Manager.
 - When using the PPM installed on a Cisco IAC Management Appliance, the user name is “cisco”.
 - When using a standalone PPM server or when a new account has been created on the Cisco IAC Management Appliance for the server connection, the user name will be as set by the PPM administrator.

- Enter the **Password** assigned to the account used to connect to Cisco Prime Performance Manager.
 - When using the PPM installed on a Cisco IAC Management Appliance, this must be the same password that was entered for the “Administrator Password” property during the installation procedure for the Cisco IAC Management Appliance.
 - When using a standalone PPM server or when a new account has been created on the Cisco IAC Management Appliance for the server connection, the password will be as set by the PPM administrator.
 - Re-enter the password to confirm it.
6. Click **Submit Order**.

Defining the Cisco Process Orchestrator Platform Element

You must be logged in as the Cloud Provider Technical Administrator to perform this task. Complete the following steps to define the connection information for Cisco Process Orchestrator that will be used in Cisco Intelligent Automation for Cloud 4.2.

1. Launch Cisco Intelligent Automation for Cloud 4.2 and log in as a Cloud Provider Technical Administrator.
2. Choose **Setup > System Settings > Connections** tab.
3. On the Connections tab, click **Connect Cloud Infrastructure** to open the form.
4. On the Connect Cloud Infrastructure form, choose Cisco Process Orchestrator from the Choose Platform Element area’s Platform Element Type drop-down list.
5. In the Cisco Cloud Portal area, specify the following connection information:
 - Enter the **Connection Name**. This is the “friendly name” for the Cisco Process Orchestrator connection.
 - Enter the **Host Name**. This is the host name or IP address for Cisco Process Orchestrator.
 - Enter the **Request Center Port**. By default, this is 8080.
 - Enter the **Service Link Port**. By default, this is 6080.
 - *Optional*. Enter information that describes Cisco Process Orchestrator.
 - Click the **True** or **False** radio button to indicate whether the connection is encrypted. *False* is chosen by default.
 - Enter the **Service Link URL**.
 - Enter **NSAPI User Name** to use when connecting to the Cisco Process Orchestrator server.
 - Enter **NSAPI Password** assigned to the account used to connect to the Cisco Process Orchestrator server.
 - Confirm NSAPI Password.

Note: NSAPI is an account to connect Cisco Process Orchestrator to Cisco Prime Service Catalog.
6. In the Cisco Process Orchestrator area, specify the following connection information:
 - Enter the **Connection Name**. This is the “friendly name” for the Cisco Process Orchestrator connection.
 - Enter the **Host Name**. This is the host name or IP address for Cisco Process Orchestrator.
 - Enter the **Port**.
 - Enter the **URL**.

- Enter the **Administrator User Name**.
 - Enter the **Administrator User Domain**.
 - **Connection Encrypted**. Click the **True** or **False** radio button to indicate whether the connection is encrypted. *False* is chosen by default.
7. Click **Submit Order**.

Defining the Cisco Unified Computing System (UCS) Director Platform Element

You must be logged in as the Cloud Provider Technical Administrator to perform this task. Complete the following steps to define the connection information for Cisco UCS Director that will be used in Cisco IAC 4.2.

1. Launch Cisco Intelligent Automation for Cloud 4.2 and log in as a Cloud Provider Technical Administrator.
2. Choose **Setup > System Settings > Connections** tab.
3. On the Connections tab, click **Connect Cloud Infrastructure** to open the form.
4. On the Connect Cloud Infrastructure form, choose **Cisco UCS Director** as the Platform Element Type.
5. Specify the following connection information for Cisco UCS Director:
 - Enter the **Connection Name**. This is the “friendly name” for the Cisco UCS Director connection.
 - Enter the **Host Name**. This is the host name or IP address for Cisco UCS Director.
 - *Optional*. Enter information that describes Cisco UCS Director.
 - Click the **True** or **False** radio button to indicate whether secure connection protocol is used to connect to the server. *True* is chosen by default.
 - Click the **True** or **False** radio button to indicate whether certificate error messages should be ignored. *True* is chosen by default.
 - Enter the **User Name** to use when connecting to Cisco UCS Director.
 - Enter the **Password** assigned to the account used to connect to Cisco UCS Director.
 - Re-enter the password to confirm it.
6. Click **Submit Order**.

Defining the Cisco UCS Manager Platform Element

You must be logged in as the Cloud Provider Technical Administrator to perform this task. Complete the following steps to define the connection information for the Cisco UCS Manager that will be used in Cisco Intelligent Automation for Cloud 4.2.

1. Launch Cisco Intelligent Automation for Cloud 4.2 and log in as a Cloud Provider Technical Administrator.
2. Choose **Setup > System Settings > Connections** tab.
3. On the Connections tab, click **Connect Cloud Infrastructure** to open the form.
4. On the Connect Cloud Infrastructure form, choose **Cisco UCS Manager** from the Platform Element Type drop-down list.
5. Specify the following connection information for the Cisco UCS Manager server:
 - Enter the **Host Name** or IP address for the Cisco UCS Manager server. For example: *test-ucs-000.domain.local*

Connecting the Cloud Platform Elements

- Enter the TCP/IP port used to connect to the Cisco UCS Manager server. By default, the following ports are used:
 - Port 443—SSL protocol
 - Port 80—HTTP connection
 - *Optional.* Enter information that describes the Cisco UCS Manager server.
 - Choose the time zone that is used on the Cisco UCS Manager server from the drop-down list.
 - Click the **True** or **False** radio button to indicate whether secure connection protocol is used to connect to the server. *True* is chosen by default.
 - Click the **True** or **False** radio button to indicate whether certificate error messages should be ignored. *True* is chosen by default.
 - Click the **True** or **False** radio button to indicate whether Cisco UCS Manager is **Managed by Cisco UCS Director**. *False* is chosen by default.
Note: In you choose **True** you are prompted to enter two additional settings: **Cisco UCS Director Instance** and **Cisco UCS Director Physical Account**.
 - Enter the **User Name** to use when connecting to the Cisco UCS Manager server.
 - Enter the password assigned to the account used to connect to the Cisco UCS Manager server.
 - Re-enter the password to confirm it.
6. Click **Submit Order**.

Defining the OpenStack Cloud Manager Platform Element

You must be logged in as the Cloud Provider Technical Administrator to perform this task. Complete the following steps to define the connection information for the OpenStack Cloud Manager that will be used in Cisco Intelligent Automation for Cloud 4.2.

1. Choose **Setup > System Settings > Connections** tab.
2. Click **Connect Cloud Infrastructure**.
3. On the Connect Cloud Infrastructure form, choose **OpenStack Cloud Manager** from the Platform Element Type drop-down list.
4. Specify the following connection information for the OpenStack Cloud Manager server:
 - Enter the **Connection Name**. This is the “friendly name” for the OpenStack Cloud Manager connection.
 - Enter the **Host Name**. This is the host name or IP address for the OpenStack Nova Compute.
 - Enter the **Port**. This is the TCP/IP port used to connect to the OpenStack Nova Compute. By default, the following Port 8774 is used.
 - Click the **True** or **False** radio button to indicate whether **Secure connection** protocol is used to connect to the server. *True* is chosen by default.
 - Click the **True** or **False** radio button to indicate whether **certificate error messages** should be ignored. *True* is chosen by default.
 - Set the APIC Enabled OpenStack option to **Yes** if the OpenStack deployment is enabled with the APIC plug-in.
 - If set to **Yes**, you then select the Cisco APIC to be used.

- Enter the **Keystone Port**, which is the TCP/IP port used to connect to the keystone authentication.
Note: By default, port 5000, the Public URL endpoint port, is set. Alternatively, you can specify the AdminURL port 35357.
 - Enter the account **User Name** to use when connecting to the OpenStack Cloud Manager server.
 - Enter a **Project Name**. Enter the Project Name for which system administrator have the access rights. This Project name is used only to acquire authentication token for the operations. If no Project Name is provided, the user name will be used as the tenant name by default.
 - Enter the **Password** assigned to the account used to connect to the OpenStack Cloud Manager server.
 - Re-enter the password to confirm it.
5. Click **Submit Order**.

Defining the Puppet Platform Element

You must be logged in as the Cloud Provider Technical Administrator to perform this task. Complete the following steps to define the connection information for the Puppet platform element that will be used in Cisco Intelligent Automation for Cloud 4.2.

1. Launch Cisco Intelligent Automation for Cloud 4.2 and log in as a Cloud Provider Technical Administrator.
2. Choose **Setup > System Settings > Connections** tab.
3. On the Connections tab, click **Connect Cloud Infrastructure** to open the form.
4. On the Connect Cloud Infrastructure form, choose **Puppet** from the Platform Element Type list.
5. Specify the following connection information for the Puppet platform element:
 - Enter the **Connection Name**. This is the “friendly name” for the Puppet platform element connection.
 - *Optional.* Enter information that describes the Puppet platform element.
 - Enter the **Host Name**. This is the host name or IP address for the Puppet platform element.
 - Enter the **SSH Login** and the **SSH Password** assigned to the account used to connect to the Puppet platform element.
 - Re-enter the SSH Password to confirm it.
 - Enter the **Private Key**. (This is Optional. Not all deployments require this.)
6. Check the **Show Additional Options** check box (*optional*). Here you can add additional information such as:
 - **Installer Package Base URL**. This is the Base URL for downloading the Puppet Enterprise installer package. Default location is PuppetLabs repository. This can also be a local HTTP resource where installer packages are stored.
 - **Alternate Module Path**. By default, discovery uses the modulepath as defined in puppet.conf. You can point discovery to an alternate path such as a GIT working copy. In defining an alternate path, you can use **\$environment** to dynamically insert the environment in the path.
 - **Hiera Node Classification Path**
Note: New nodes are classified using Hiera Yaml files, and, by default, are saved to the Puppet Master location specified by the first folder specified in the module path. These files can be stored in an alternate location, perhaps separate from your modules. In defining the hiera path, you can use **\$environment** to dynamically insert the environment in the path. Remember, this location must match what is defined in your hiera.yaml file in the Puppet Master’s configuration directory.

- Set up **Linux Proxy**.
 - Set up **Linux Proxy Bypass**.
 - Enter the **Linux Bootstrap User** and **Linux Bootstrap Password**.
 - Set up **Windows Proxy**.
 - Set up **Windows Proxy Bypass**.
 - Enter the **Windows Bootstrap User** and **Windows Bootstrap Password**.
7. Click **Submit Order**.

Defining the Connection Information for VMware vCenter Platform Element

Complete the following steps to define connection information for VMware vCenter.

1. Launch Cisco Intelligent Automation for Cloud 4.2 and log in as a Cloud Provider Technical Administrator.
 2. Choose **Setup > System Settings > Connections** tab.
 3. On the Connections tab, click **Connect Cloud Infrastructure** to open the form.
 4. On the Connect Cloud Infrastructure form, specify the following connection information for the network services manager:
 - Enter the **Connection Name**. This is the “friendly name” for the VMware vCenter element connection.
 - Enter the **Host Name**. This is the host name or IP address for the Puppet platform element.
 - Enter the TCP/IP **Port** used to connect to the VMware vCenter. by default, port 443 is used.
 - *Optional*. Enter information that describes the VMware vCenter.
 - Click the **True** or **False** radio button to indicate whether secure connection protocol is used to connect to the server. *True* is chosen by default.
 - Click the **True** or **False** radio button to indicate whether certificate error messages should be ignored. *True* is chosen by default.
 - Click the **True** or **False** radio button to indicate whether VMware vCenter is **Managed by Cisco UCS Director**. *False* is chosen by default.
- Note:** In you choose **True** you are prompted to enter two additional settings: **Cisco UCS Director Instance** and **Cisco UCS Director Physical Account**.
- Enter the **User Name** to use when connecting to the VMware vCenter Server.
 - Enter and re-enter the **Password** assigned to the account used to connect VMware vCenter server.
5. Click **Submit Order**.

Defining Connection Information for VMware vCloud Director Platform Element

Complete the following steps to define connection information for VMware vCloud Director.

1. Launch Cisco IAC 4.2 and log in as a Cloud Provider Technical Administrator.
2. Choose **Setup > System Settings > Connections** tab.

3. On the Connections tab, click **Connect Cloud Infrastructure** to open the form.
4. On the Connect Cloud Infrastructure form, specify the following connection information for the network services manager:
 - Enter the **New Connection Name**. This is the “friendly name” for the VMware vCloud Director element connection.
 - Enter the **Host Name**. This is the host name or IP address for the VMware vCloud Director platform element.
 - *Optional*. Enter information that describes the VMware vCloud Director.
 - Click the **True** or **False** radio button to indicate whether certificate error messages should be ignored. *True* is chosen by default.
 - Enter the **User Name** to use when connecting to the VMware vCloud Director server.
 - Choose the **Domain** type, either **System** or **Organization**. In you choose **Organization**, you are prompted to enter the **Organization Name**. (The connection to vCloud Director is “UserName@System.”)
 - Enter and re-enter the Administrator **Password** assigned to the account used to connect VMware vCloud Director server.
5. Click **Submit Order**.

Setting Provisioning Settings

Specify the settings for bare metal and virtual machine provisioning, then verify that the bare metal and virtual machine provisioning settings are configured correctly.

1. Choose **Setup > System Settings > System Settings** tab.
2. On the System Settings tab, click **Set Provisioning Settings**.
3. On the Server Provisioning Settings form, specify the following:

Set Provisioning Settings

- **Default VMware vCenter Clone Timeout (Minutes)**. Enter the period of time allowed, specified in minutes, before a virtual machine deployment operation is determined as failed.
- **Duplicate Alert Suppression Time period (Hours)**. Enter the amount of time, in whole hours, to suppress duplicate alerts related to cloud automation.
- **CloudSync Discovery Interval (Hours)**. The amount of time, in whole hours, between consecutive periodical executions of the CloudSvnc infrastructure discovery service.
- **CloudSync Discovery Timeout (Minutes)**. Enter the period of time allowed, specified in minutes, before a CloudSvnc Discovery operation is determined as failed.
- **Collect Metrics Interval (Hours)**. The amount of time, in whole hours, between consecutive periodical executions of the collect metrics process.
- **System Health Check. Setting for performing platform element connection validation services. (ON or OFF)**
- **Cloud Domain**. Enter the domain name.
- **Cloud Domain User**. Enter the cloud domain user name.
- **Cloud Domain Password**. Enter the domain user's password.

Note: You can now set *multiple* domains. See [Setting Multiple Domains, page 59](#) for details.

- **Verify Cloud Domain Password.** Re-enter the domain user's password.
- **Cloud Default Time Zone Linux.** Choose the default time zone for Linux.
- **Cloud Default Time Zone Windows.** Choose the default time zone for Windows.
- **Order Status History Cleanup.** Choose Yes/No for enabling/disabling Order Status History Cleanup.
- **System Health History Grooming.** Choose Yes/No for enabling/disabling System Health History Grooming.

Network Services Settings

4. Enter the following in the Network Services Settings section:

- **NTP Server.** Be sure NTP server entered matches up with the Server Configured Network services controller.
- **Routing Protocol.** Choose a Routing Protocol to be used for routing external network traffic.
- **Process Orchestrator Network (subnet).** Enter network address for configuring the static route between virtual network devices and Cisco Process Orchestrator.
- **Process Orchestrator Network (subnet mask).** Enter subnet mask for configuring the static route between virtual network devices and Cisco Process Orchestrator.
- **Cisco Adaptive Security Appliance Image.** Choose an image from the list to be used for provisioning Cisco Adaptive Security Appliance.
- **Cisco Cloud Services Router Image.** Choose an image from the list to be used for provisioning Cisco Cloud Services Router.
- **Cisco Prime Network Services Controller Image.** Choose an image from the list to be used for provisioning Cisco Prime Network Services Controller image.
- **Cisco Virtual Security Gateway Image.** Choose an image from the list to be used for provisioning Cisco Virtual Security Gateway.
- **Netscaler 1000v Load Balancer Image.** Choose an image from the list to be used for provisioning Citrix Netscaler 1000v Load Balancer Image.
- **IP Address Source.** Specifies whether IP Address Management will be handled by the Service Portal or by an External IPAM system.
- **Username** is entered by the system.
- Enter the **Password** and re-enter the password.
- **WAN Router(s).** When enabled, the system will require ASN and BGP configuration information for a pair of ASRs, operating in an HA cluster. Options are Single ASR, HA Cluster, and Standalone.
- **Ping Sweep.** Controls whether ICMP echo requests are sent to every IP address within a subnet range as networks are added to the system. When an ICMP response is received, the corresponding IP address will be marked as assigned.

Single or HA Cluster Details

5. In the **Single or HA Cluster Details** section (the necessary network settings used to create Advanced Network Services), enter the following:
- **Provider Internet AS Number.** Enter Autonomous System Number (ASN) for Internet Network.
 - **Provider Enterprise AS Number.** Enter Autonomous System Number (ASN) for Enterprise Network.

- **Tenant AS Number.** Enter Autonomous System Number (ASN) for Tenant Network.
- **Enter the Internet Gateway.**
- Enter the **Internet Remote BGP Peer IP.**
- **Enterprise Transit IP Space.** Enter the network for this subnet in CIDR notation. For example, 192.168.20.0/24. Enter only an IPv4 type of IP address.

Note: This only networks from /23 through /29 are supported.

- **Enterprise Gateway.** The IP address of the gateway router interface that will be used as the next hop for traffic leaving the VDC's destined for the Enterprise.
- **Enterprise Remote BGP Peer IP.** The IP address used for BGP peering by the gateway router for advertising routes to the Enterprise.

Standalone ASR Details

6. In the **Standalone ASR Details** section (which appears only if you choose "Standalone" from the WAN Routers(s) drop-down), enter the following:
 - **Provider Internet AS Number.** Enter Autonomous System Number (ASN) for Internet Network.
 - **Provider Enterprise AS Number.** Enter Autonomous System Number (ASN) for Enterprise Network.
 - **Tenant AS Number.** Enter Autonomous System Number (ASN) for Tenant Network.
 - Enter the **Internet Gateway.**
 - Enter the **Internet Remote BGP Peer IP.**
 - **Enterprise Transit IP Space.** Enter the network for this subnet in CIDR notation. For example, 192.168.20.0/24. Enter only an IPv4 type of IP address.

Note: Only networks from /23 through /29 are supported

 - **Enterprise Gateway.** The IP address of the gateway router interface that will be used as the next hop for traffic leaving the VDC's destined for the Enterprise.
 - **Enterprise Remote BGP Peer IP.** The IP address used for BGP peering by the gateway router for advertising routes to the Enterprise.
7. Click **Submit Order.**

Setting Multiple Domains

With the Cisco IAC 4.2 Multiple Domains feature, *new for 4.2*, you now have the ability to setup different domains for every tenant, organization and virtual data center.

To work with multiple domains, start Cisco IAC and login as a CPTA. Then follow the steps below.

Registering Domains

1. Go to **Setup > System Settings**.
2. From the System Settings tab, choose **Register Domain**.
3. On the Register Domain form, complete the following:
 - a. **Domain Name**: Enter the domain name to register.
 - d. **User Name**: Enter the user name to register.
 - e. **Password**: Enter the password for this domain.
 - f. **Confirm Password**: Re-enter the password for this domain.
4. Click **Submit Order**.

Updating Domains

1. Go to **Setup > System Settings**.
2. From the System Settings tab, choose **Update Domain**.
3. On the Update Domain form, complete the following:
 - a. **Domain Name**: Select the domain name.
 - b. **User Name**: Select, modify, or enter the user name to register.
 - c. **Password**: Enter the password for this domain.
 - d. **Confirm Password**: Re-enter the password for this domain.
4. Click **Submit Order**.

Removing Domains

1. Go to **Setup > System Settings**.
2. From the System Settings tab, choose **Remove Domain**.

Note: All of the dependencies on this domain (organizations, tenants, VDCs, etc) must be removed prior to this step.
3. On the Remove Domain form, complete the following:
 - a. **Domain Name**: Select the domain name.
 - b. **Confirmation**: Check **Yes**.
4. On the popup, click **OK** to confirm.
5. Click **Submit Order**.

Adding or Removing Tenant Domains

1. Go to **Setup > System Settings**.
 2. From the System Settings tab, choose **Add or Remove Tenant Domains**.
 3. On the Add or Remove Tenant Domains form, complete the following:
 - a. **Provider Name:** The provider name automatically populates.
 - b. **Tenant Name:** Choose the tenant name. Any VMs ordered under the tenant will use the domain.
 4. Choose one of the two radio buttons:
 - **Add Domain:** To add multiple domains to Tenant/Organization.
 - **Remove Domain:** To remove a domain associated to selected Tenant/Organization. If you choose this option, another field will appear, displaying the list of available domains for you to select from for the deletion.
- Note:** Optionally, you can use the **Organization Name** field to also add this domain automatically to an organization, along with the Tenant Name.
5. Click **Submit Order**.

Note: If you select to add to a tenant and an organization, it will be added to both, first to the tenant and then to the organization, saving you some work.

Note: When you remove a domain and have an Organization selected, the domain will only be removed from the Organization and not from the Tenant. But when you *add* a domain, it is added to both the Organization and the Tenant.

Note: If the Tenant or Organization has multiple domains associated with it (even if just two), then one of the domains from the list of many domains will be selected. To make sure only one is selected, be sure to add the domain to the VDC or have only one domain be part of an Organization or Tenant, whichever level is lowest.

Note: When you create or modify an organization (Management > Tenant Management > Tenants and Organizations), you will find the same options and radio buttons as described above.

Note: VMs will first select the domain associated to a VDC. If VDC has no domain associated with it, then it will select a Domain from the Organization list. If neither VDC nor Organization have a domain, then a Tenant Domain is selected. If none of those options are available, the VM will get the default domain from the Provider as set in Provisioning Settings.

Note: You select Organization/Tenant/Provider Domains. Initially, the list shows the VDC - Organization Domains to select. However, if Organization Domains are not there, then VDC - Tenant Domains will display. Finally, if Tenant Domains are not there, then Provider Domains will be shown.

Note: VDC can only have one domain associated with it which it can be added from My VDCs > Create Virtual Data Center. For options in domains, the Organization to which this VDC will belong to should have domains associated with it.

Note: To remove the domain association to VDC you need to first decommission the VDC.

Setting System-Wide Service Options

Use the Set System-Wide Service Options service to control what ordering options are available to users in Cisco IAC by globally enabling or disabling the following Cisco IAC services:

- Virtual Machine From Template Ordering
- Community VDC Ordering
- Application Configuration Management
- Physical Server Ordering

Setting System-Wide Service Options

- Virtual Machine Ordering
- Install OS Ordering
- Service Assurance
- Virtual Data Center Ordering
- Advanced Network Services (IAC Management Appliance and Cisco Nexus 1000v required)
- Multiple Security Zones
- Enhanced VM Security
 - High Availability (Enhanced VM Security only)
- Load Balancing Services

These settings affect all clients across all tenants and cannot be configured at tenant-level.

Before enabling each of the service options, make sure the following prerequisite configuration steps are performed:

Step	Requirement	Configuration Steps
Create a virtual datacenter	<ul style="list-style-type: none"> ■ vCenter platform element is registered ■ POD is created 	<ul style="list-style-type: none"> ■ Register Datastores ■ Create networks
Community VDCs	<ul style="list-style-type: none"> ■ vCenter platform element is registered ■ POD is created 	<ul style="list-style-type: none"> ■ Register Datastores ■ Create networks
Order VM from Template	<ul style="list-style-type: none"> ■ VM templates created and discovered ■ Virtual Data Center or Community VDC is created 	<ul style="list-style-type: none"> ■ Register Virtual Machine templates

1. Choose **Setup > System Settings > System Settings** tab.
2. On the System Settings portlet, click **Set System-wide Service Options**.
3. On the Set System-wide Service Options form, choose **YES** or **NO** the following options:
 - a. Virtual Machine From Template Ordering
 - b. Virtual Machine Ordering
 - c. Community VDC Ordering
 - d. Virtual Data Center Ordering
 - e. Advanced Network Services
 - f. Multiple Security Zones
 - g. Enhanced VM Security
 - High Availability

Note: High Availability is an option under Enhanced VM Security. If Enhanced VM security is set to No, you will not see the High Availability option.

- h. Service Assurance
- i. Application Configuration Management
- j. Load balancing Services

4. Click **Submit Order**.

When a service is disabled, users (Organization Technical Administrators and Server Owners) are prevented from ordering from the portal or portlet, and from submitting service forms from the My Services module. Although users can see the portal or portlet of the disabled service, a “disabled” message displays, and “Submit” buttons are hidden on the service forms. Disabling an option only affects what clients can order from the catalog from the time the Set System Wide Service Options service order is fulfilled. It does not affect current, active services that have already been ordered. You can re-enable a disabled service at any time.

1. Choose **Setup > System Settings > System Settings** tab.
2. Click **Set System-wide Service Options** to open the form.
3. Disable a service by clicking the **No** radio button, or re-enable a disabled service by clicking the **Yes** radio button.
4. Click **Submit Order** to send the order, close the form, and display the order confirmation.

Registering a Datastore

Datastores that are discovered automatically during Connect Cloud Infrastructure must be registered before they can be used in the VDC community and organization virtual data centers. A single datastore can be used by one or more Virtual Data Centers.

1. Choose **Setup > Manage Infrastructure**.
2. Choose **Datastores** in the VMware vCenter resources. Discovered datastores for the VMware vCenter will be shown.
3. Choose a datastore with a status of Discovered that should be registered for use.
4. Click **Register**. This starts the Register Datastore service.
5. Enter a display name and description for the Datastore (optional).
6. Click **Submit Order**.

Setting Up REX and nsAPI User Accounts

This section guides you through how to create user accounts for REX adapter and nsAPI that will be used to connect Prime Service Catalog to the REX adapter and Process Orchestrator, respectively.

Note: You created at least one nsAPI username and password when you imported and configured Cisco Intelligent Automation for Cloud into Prime Service Catalog.

Setting Up A REX User Account

1. Choose **Organization Designer** from the module drop-down list.
2. On the Organization Designer home page, click **Create Person** in the Common Tasks pane.

Setting Up REX and nsAPI User Accounts

Note: If you are using directory integration, the local password of the REX user must match the directory integration password. To do so, log in with REX user; a local account will be created. Then, go to Organization Designer and update the password of the REX user to match the directory integration password. Note that the timezone for these users need to be GMT (Greenwich Mean Time).

3. Set up the REX user account:

Note: You may only set up REX user account as a local account; If you're using directory integration, the REX user account will still be from a local source.

4. On the Create Person form, provide the necessary information.

5. Click **Create** to submit and close the form.

When the form closes, the People portal displays, showing the user information you just entered. If you need to make corrections, make them before proceeding to the next step.

6. Click **Add** in the upper right corner to add the REX user account.

Configuring Agent Properties

There are two new Agent types: DB and NSAPI. To configure agent properties for all REX agents and DB/HTTP/NSAPI agents, refer to the following sections:

- Set username and password for the “REX Set REX Agent Properties” agent
- Start “REX Set REX Agent Properties” agent
- Set REX Agent Configuration
- Start All REX Agents
- Setting DB, HTTP, NSAPI Agents Configuration
- Start all other agents

Setting Username and Password for REX Set REX Agent Properties

1. Choose **Service Link** from the module drop-down list.
2. Click the **Manage Integrations** tab along the top left of the screen.
3. In the Agents pane on the left, expand **REX Set REX Agent Properties** (you will most likely need to scroll down) and click **Outbound Properties**.
4. In the **REXOutboundAdapter.Username** field, enter the REX login name that you created in the Create Person form.
5. In the **REXOutboundAdapter.Password** field, enter the REX password in the Create Person form.
6. Click **Save**.

Starting the REX Set Agent Properties Agent

1. Choose **Service Link** from the module drop-down list, then click the **Control Agents** tab to open the portal. The Control Agents portal displays a list of all agents.
2. Click the **red icon** next to **REX Set REX Agent Properties**, then click **Start Chosen**.

Note: If you do not see REX Set REX Agent Properties in the list, do one of the following:

- scroll down
- use the page buttons to go up and down the list or to enter a specific page number
- sort by agent name by clicking the Name column heading.

The red icons turn to green, indicating that they are now sending and receiving.

Setting REX Agent Configuration

Configure all of the REX agent properties, then verify that the agents are configured correctly.

1. Choose **Setup > System Settings > System Settings** tab.
2. On the Agent Properties Configuration portlet, click **Set REX Agent Configuration**.
3. The Set REX Agent Configuration form displays.
4. On the Set REX Agent Configuration form, enter the REX account login name, then enter and re-enter the REX account password.
5. Enter the URL to the Prime Service Catalog Request Center server in the **Prime Service Catalog Request Center URL** field. The URL should include http or https, the hostname and port number, and the pathname to RequestCenter. For example, http://localhost:8080/RequestCenter.
6. Click **Submit Order** to submit the form and display the Order Confirmation page for the service that you ordered. **Do not close the order confirmation.**
7. In the Requisition Details pane, click the requisition number to open the requisition summary page.
8. Click **Comments & History** in the menu on the right side of the window.
9. In the System History pane, look for errors.

Note: If the REX agents are configured correctly, you will see a message for each agent stating that it was updated successfully.

10. Close the Comments and History window.

Starting All REX Agents

1. Choose **Service Link** from the module drop-down list, then click the **Control Agents** tab to open the portal. The Control Agents portal displays a list of all agents.
2. Choose each of the following REX agents:
 - a. REX Add Organization Unit
 - b. REX Add Organization Unit (Tenant)
 - c. REX Add Person
 - d. REX Create Queue
 - e. REX DeactivateOU
 - f. REX Delete Queue
 - g. REX Modify Organization Unit
 - h. REX Set DB Agent Properties
 - i. REX Set HTTP Agent Properties

j. REX Set NSAPI Agent Properties

Note: If you do not see any REX agents in the list, scroll down. Or, sort by the agent name by clicking the **Name** column heading.

3. Click **Start Chosen**. (This button is located on top right of the screen.)
4. Refresh the screen by clicking **Refresh** (on the navigation buttons near the bottom right of the screen).

The agents become green after you refresh.

Setting DB, HTTP, NSAPI Agents Configuration

Follow the steps below to configure DB, HTTP, and NSAPI agents.

Note: All three agent types (DB, HTTP, NSAPI) need to be configured.

1. Choose **Setup > System Settings > Connections** tab.
2. Click **Set Agent Configuration** to open the form.
3. On the Set Agent Configuration form, choose an Agent Type, then provide the required information.
4. When you are done, click **Submit Order** to submit the form and display the Order Confirmation page for the service that you ordered. Do not close the order confirmation.
5. In the Requisition Details pane on the Order Confirmation page, click the requisition number.
6. On the Requisition Summary page, click **Comments & History** in the menu on the right side of the window.
7. In the System History pane on the Comments and History page, look for errors.
Note: If the agents were configured correctly, you will see a message that the agent was updated successfully.
8. Close the Comments and History window.

Setting Up nsAPI User Account

1. On the Create Person form, provide the following information:
2. Click **Create** to close the form and return to Organization Designer.
3. In Organization Designer, choose **People** from the Search drop-down list.

In the People pane below, names display.

4. Locate and click the name of the nsAPI user.
5. From the General menu on the right side of the page, choose **Calendar**.
6. In the Calendar pane, change all time values in the **To** column to **11:59 PM**.
7. Click **Update** to submit the form.

Assigning the Cloud Technical Administrator Role to an nsAPI User

1. Choose **Setup > System Settings > Administrators**.
2. On the Cloud Administrators portlet, click **Add Cloud Administrator**.

3. On the Add Cloud Administrator form, choose Choose Existing User from the Action drop-down list.
4. Choose the nsAPI user.
5. Click **Submit Order**.

Manually Adding the Site Administrator Role to an nsAPI User

You can manually add the Site Administrator role to an nsAPI user without directory service. Follow the steps below.

1. Choose **Organization Designer** from the module drop-down list, choose the **People** tab.
2. Choose the nsAPI user.
3. Choose **Roles**, check the **Site Administrator** check box, then click **Add**.

Starting All Other Agents

1. Choose **Service Link** from the module drop-down list, then click the **Control Agents** tab.
2. While pressing and holding **Shift**, click the red icon next to the first agent in the list, then click the red icon of the last agent in the list to choose all of the agents, then click **Start Chosen**.

Note: If a vertical scroll bar appears in the list, scroll down to choose the last agent on the page.

The red icons turn to green, indicating that they are now sending and receiving.

3. If there are additional agents in the list, use the scroll arrow at the bottom of the list to display to them, then repeat Step 2, above

Setting Up a Community VDC

A community VDC (virtual data center) can be used by server owners in any organization to provision virtual and physical servers. A community VDC lives on a cluster in a POD and has datastores, resource pools, and community networks resources associated with it.

Multiple community VDCs can be created by the Cloud Provider for server owners to provision servers in. A virtual data center has an associated size that determines limits for the number of virtual servers, physical servers, vCPUs, CPU MHz, storage, and memory.

Limits are enforced by comparing the sum of the number of provisioned virtual and physical servers and the vCPUs, memory, and storage for a server size against the limits defined for the virtual data center size.

A VMware resource pool is created for each virtual data center. This allows further control of resource utilization by defining CPU and memory limits, as well as CPU and memory reservations in the VMware resource pool.

- On the Create VDC service form (**My Cloud > My VDCs**), choose “Community VDC” to create the Community VDC.

Note: If the Community VDC ordering is set to No for the chosen Tenant, then by default the Community VDC option is set to No on the form.

Adding a Server Owner

Cisco Intelligent Automation for Cloud users consist of Server Owners, who are end users of an organization who order and provision servers. There are two kinds of Server Owners:

- Virtual and Physical Server Owner—Orders and provisions virtual machines and physical servers. Defines/assigns/adds a SO after creating an organization.

- Virtual Server Owner—Orders and provisions virtual machines only.

Both users are created using the same form. To add users, complete the following steps:

1. Choose **Management > Tenant Management**.

2. Choose a Tenant.

3. Choose the Organization where the server owner is located (within the tenant).

Note: Server Owners can only be added to an Organization. Actions are allowed at the tenant level with regard to Add User are adding TTA and/or TBA. Even where the TTA and the TBA are already defined, you cannot add a Server Owner at the tenant level.

4. On the Tenant Management form, choose the Users tab.

5. Click **Add User**.

6. On the Add User form, choose the organization to which you want to add a new user as a Server Owner.

7. Choose **Create New User** from the Action drop-down list. Provide the following:

a. Enter the first and last name of the new Server Owner, a unique login identifier for the new Server Owner, and the new Server Owner's e-mail address.

b. From the drop-down list, choose the time zone of the new Server Owner's primary address.

c. Enter, then re-enter the password for the new Server Owner.

8. In the **Roles** field, click one of the following radio buttons to indicate the role to be assigned to the user:

a. Virtual Server Owner—User can order virtual servers.

b. Virtual and Physical Server Owner—User can order both virtual and physical servers.

9. Click **Submit Order**.

Assigning Mail Addresses for Queue Notifications

You must update the queue configuration settings with the e-mail addresses that will receive e-mail notifications for changes in the service queues. A queue is a repository for administrative tasks that must be performed, such as monitoring service delivery, lease instances, or failed service remediation.

Tasks are automatically added to the queue by the Cloud system. Users with permissions can see the queues, assign tasks, and take action on the tasks in Service Manager. When an organization is created, Cisco IAC creates the following approvals queue:

Approval for <Organization Name>

This queue will contain tasks that are waiting for approval by the Organization Technical Administrator.

Cloud Provider Technical Administrators (CPTAs) and Organization Technical Administrators (OTAs) can monitor, assign, or address tasks added to the queues. Those users with access to the queues can perform the tasks added to the queues. When a task is added to a queue or is assigned or reassigned to a user, the designated users receive e-mail notifications.

To prepare the queues for use, you must specify the e-mail addresses of the users who receive e-mail notifications when a task is added to a queue.

Note: *If you skip this task, no one will receive notifications of changes to the queues. Use mailing lists (aliases), not specific user e-mail addresses. You must configure e-mail addresses for each queue.*

1. Launch Cisco Intelligent Automation for Cloud and log in as a Site administrator.
2. Choose **Organization Designer** from the module drop-down list, then click the **Queues** tab.
3. In the Queues pane, click **Approvals for <Organization Name>**.
4. From the menu on the right side of the window, click **Contact** to display the Contact pane.
5. Click **Add New** button, choose e-mail as the Type and enter the e-mail address in the value field.
6. Click **Update**.



Managing Organizations and Users

Understanding Organizations

Organizations are users who are grouped according to function or business. There are two kinds of organizations: business units and service teams. Note that new cloud infrastructure for advanced network services are provisioned and dedicated on a 'per Organization' basis. Organizations fit within the overall logical construct of Cisco IAC.

Organizations

Organizations are groups of end users who order services. The typical business unit represents a department or group with a specific purpose—for example, marketing—that has an interest in maintaining separate servers from other groups. This type of organization represents the majority of organizations in the cloud system. Business units include the following types of users:

- Organization Technical Administrator ([Organization Technical Administrator, page 33](#))
- Virtual Server Owner ([Virtual Server Owner, page 34](#))

Service Teams

Service teams are units whose members administer and maintain the Cisco IAC solution, which includes Prime Service Catalog. Service teams typically include employees of the service provider who are Cloud Provider Technical Administrators and Site Administrators. Cisco technicians might also be part of service teams. The Cloud Provider Technical Administrator is a member of the CPTA Organization Unit service team.

Working with Organizations

To create an organization or view details on an existing organization, such as number of users and lists of organization administrators and accessible networks/VLANs, use the Tenant Management feature. New cloud infrastructure for advanced network services are provisioned and dedicated on a per Organization basis.

Note: Cisco IAC supports an individual's membership to a single organizational unit or membership (not multiple).

Creating an Organization

1. Choose **Management > Tenant Management**.
2. On the Tenant Management page, Choose a specific Tenant to which you want to add an Organization.
3. Click **Create Organization**.
4. On the Create Organization form, under the General Organization Information heading, enter:
 - Organization Name. Organizations may not contain forward slashes.
 - Organization Description.
 - Organization Name to be Created (entered by the system)
5. Choose VDC Connection Type.

6. To set Organization-wide Service Options, choose Yes or No for the following options:

Note: The list below are the “service offerings” as set by the CPBA tenant-wide. These settings may or may not be selectable depending on the service offerings of the tenant to which the organization pertains.

- Virtual Machine From Template Ordering
- Physical Server Ordering
- Install OS Ordering
- Community VDC Ordering
- Application Configuration Management
- Service Assurance
- Virtual Data Center Ordering
- Advanced Network Services
- Multiple Security Zones
- Enhanced VM Security
- Load Balancing Services

Note: If you choose Yes for Load Balancing Services, you then enter additional information.

7. Under Service Resource Container, choose the **Resource Name**. The system then automatically displays all associated information, such as:

- Compute POD Name

Note: In the case of a Compute POD configured for vCenter, you can also select a specific cluster and datastore per Service Resource Container.

- Management Network
- Service Network
- Internet Transit Network

Note: Under Application Management, you will see the server in use.

8. Click **Submit Order**.

Modifying the Cloud Administration Organization

When the cloud is first set up, the very first CPTA is defined by cloud administrator who is setting up the entire system. Later, as/if additional CPTAs need to be added (or existing CPTAs deleted), this is then done by an existing CPTA.

1. Choose **Setup > System Settings > Administrators** tab.
2. On the Administrators portlet, click Modify Cloud Administration Organization.
The **Modify Cloud Administration Organization** form displays.
3. Click **Submit Order**.
4. Review and close the information window that displays next.

Adding Cloud Provider Technical Administrators

Adding a Cloud Administrator From a New User

If you are using a directory service to import the Cloud Administrator, see the information in the following section, [Adding Cloud Administrators in the Directory Service \(If Applicable\)](#), page 1-5.

1. Choose **Setup > System Settings > Administrators** tab.
2. On the Administrators page, click Add Cloud Administrator.
3. On the Add Cloud Administrator form, choose Create New User from the Action drop-down list. The fields for creating a new user as a Cloud Administrator display.
 - Enter the first and last name of the new Cloud Administrator.
 - Enter a unique login identifier for the Cloud Administrator.
 - Enter the new Cloud Administrator's e-mail address.
 - Choose the time zone associated with the new Cloud Administrator's primary address.
 - Enter then re-enter the password for the new Cloud Administrator.
4. Click **Submit Order**.
5. To create additional Cloud Administrators, repeat [Step 5](#) through [Step 8](#).

Adding a Cloud Administrator From an Existing User

1. Choose **Setup > System Settings > Administrators** tab.
2. On the Administrators page, click Add Cloud Administrator.
3. On the Add Cloud Administrator form, choose Choose Existing User from the Action drop-down list.
4. Choose a user.
5. Click **Submit Order**.

Creating a New User to Add as an Organization Technical Administrator

If you are not using a directory service, complete the following steps to assign an existing user as an Organization Technical Administrator for an organization. This action can be performed by a CPTA, a TTA, and/or an OTA. Only a CPTA, a TTA, or an OTA can create an OTA. However, an OTA can create for his/her own organization *only*. Organization Technical Administrators are employees of the organization with some administrative access and control over their organization's environment.

Note: Organization Technical Administrators manage an organization's user accounts, virtual data centers, and organization-specific service catalogs in Cisco IAC. They also add Server Owners, or users, within the organization.

1. Choose **Management > Tenant Management**.
2. On the Tenant Management page, choose the organization to which you want to add the new user as an Organization Technical Administrator.
3. Choose **Create New User** from the Users tab and provide the following:

Removing an Organization

- Enter the user's first and last name.
 - Enter a unique login identifier for the user.
 - Enter the user's primary e-mail address.
 - Choose the time zone of the user's primary physical location.
 - In the Roles field, choose OTA.
 - Create, then re-enter a password for the user.
4. Click **Submit Order**.

Removing an Organization

Note: An Organization Technical Administrator (OTA) cannot remove an organization. Only his/her Tenant Technical Administrator (TTA) can do so.

1. Choose **Management > Tenant Management**.
2. Choose the tenant on the left side.
3. Drill down to the list of organizations associated with this tenant. (It could be just one.)
4. Choose Remove Organization icon at the bottom of the screen.
5. Verify that all information is correct.
6. Check the **Confirmation** Yes check box on the Remove Organization form.
7. Click **Submit Order**.

Creating and Managing Users

The sections that follow provide information and instructions for adding, modifying, and removing a user from an organization. Note that Cisco IAC supports an individual's membership to a single organizational unit or membership (not multiple). There is always a 1-to-1 relationship between user and tenant and the organization to which they are assigned.

Modifying User Properties

1. Choose **Management > Tenant Management**.
2. Choose the **User** tab.
3. On the left choose **Tenant/Org**.
4. From the list on the right, click the **gear** icon  next to the user you want to edit.
5. From the popup, choose **Modify User Properties**.

The user's current information appear.

- Optional. Update the email.
- Mandatory choose user role.

Note: A TTA administrator is able to demote a TTA/TBA user and change his role to OTA, VSO, or VPSO. In that case, you are prompted to choose an organization under this tenant.

6. Click **Submit Order**.

Adding User Details

1. Choose **Management > Tenant Management**.
2. Choose the **Users** tab.
3. Choose **Add User**.
4. On the Add User to the Tenant form, enter the following:
 - First Name
 - Last Name
 - Login ID
 - Email Address
 - Home Organization
 - Current Role
 - Assign Role:
 - Virtual Server Owner
 - Virtual and Physical Server Owner
 - Organization Technical Administrator
 - Tenant Technical Administrator
 - Tenant Business Administrator

At the tenant level a user can only be added as a TTA or TBA. At the Organization level a user can only be added as a VSO, VPSO, or OTA.

5. Click **Submit Order**.

Changing a User's Status to Active or Inactive

When users are created in Prime Service Catalog or imported to Prime Service Catalog from a directory service, their user status is automatically "Active." They can log in, view server details, order servers, and use other services, depending on their roles. A user whose status is "Inactive" in Prime Service Catalog can log in but cannot use the services or see server details. There are two circumstances under which a user becomes inactive:

- A Cloud Provider Technical Administrator has manually changed the user's status to inactive in Organization Designer. Thus, the user has an assigned role but is Inactive. In this case, if the user's status changed back to Active, the user's previous role and organization assignment are restored.
- The user's status was automatically changed to inactive when a Cloud Provider Technical Administrator removed the user's assigned role. Thus, the user has no assigned role and is Inactive.

Note: In this case, to change the user's status back to Active, the Cloud Provider Technical Administrator must assign a role to the user after re-activating.

1. Choose **Organization Designer** from the module drop-down list.
2. When Organization Designer page displays, click the **People** tab.
3. Use one of the following methods to locate the user:

- Use the People search field. Click the **user's name** in the search results to open the user's details.
 - Browse the list in the **People** pane to locate the user, then click the user's name to open the user's details. If the user is inactive, ensure that the Show Active Only check box is unchecked.
4. Find the Status drop-down on the General pane (upper left corner).
 5. Choose **Active** from the Status drop-down menu.
 6. Click **Update**.
 7. Respond as needed to any confirmation popup messages.

Deactivate

1. To Deactivate a user, choose **Management > Tenant Management**.
2. Choose the **Users** tab.
3. Choose the **gear** icon  next to the user you want to deactivate.
4. From the popover, choose **Deactivate User**.
5. Click **Update**.
6. Respond as needed to any confirmation popup messages.

Assigning The Role

If you have changed a user's status back to active and the user currently has no role, you must assign a role so that the user can log in and use Cisco IAC.

1. On the user's details page, click **Roles** in the menu on the right.
2. In the Roles pane, click **Add** to expand the Roles list.
3. In the Roles list, locate the role that you want to assign to the user, check the check box, then click **Add**.

Adding an Existing User as a Cloud Provider Technical Administrator

When you assign the Cloud Provider Technical Administrator (CPTA) role, the user's organization unit automatically changes to the CPTA organization, and the user's current org is removed. For example, a user belongs to an organization called "HR." If the user is added as a CPTA, the user's organization becomes the CPTA's organization. The user's membership in the HR organization is removed.

1. Choose **Setup > System Settings > Administrators** tab.
2. Choose Add Cloud Administrator to open the form.
3. On the Add Cloud Administrator form, choose **Choose Existing User** from the Action drop-down list.
4. Click **Choose** to open the Choose Person dialog box.
5. Enter the first or last (or first initial of first part of) name of the user.
6. Click **Search** to find the user.
7. In the Search Results area, click the radio button next to the name of the user.
8. Click **OK**.
9. Click **Submit Order**.

Creating a New User to Add as a Cloud Provider Technical Administrator

1. Choose **Setup > System Settings > Administrators** tab.
2. Choose Add Cloud Administrator to open the form.
3. On the Add Cloud Administrator form, choose **Create New User** from the Action drop-down list.
4. Provide the following information:
 - Enter the first and last name of the new Cloud Provider Technical Administrator.
 - Enter a unique login identifier for the Cloud Provider Technical Administrator.
 - Enter the new Cloud Provider Technical Administrator's e-mail address.
 - From the drop-down list, choose the time zone associated with the new Cloud Provider Technical Administrator's primary address.
 - Enter and then re-enter the password for the new Cloud Provider Technical Administrator.
5. Click **Submit Order**.

Removing a Cloud Provider Technical Administrator

This section describes how to remove the Cloud Provider Technical Administrator (CPTA) role from a user without deleting the user. When a user's role is removed, the user's account status is automatically changed to Inactive, and the user becomes "role-less". Inactive users can log in to Prime Service Catalog but cannot use any of its services. If you assign the user another role, you must change the user's status back to Active. See [Changing a User's Status to Active or Inactive](#), page 71.

Regulatory: All Clouds should have at least one CPTA.

1. Choose **Setup > System Settings > Administrators** tab.
2. Choose Remove Cloud Administrator to open the form.
3. On the Remove Cloud Administrator form, click **Choose** to open the Choose Person dialog box.
4. Enter the First Name or Last Name of the user, or enter a wildcard *, and click **Search**.
5. In the Search Results area, click the radio button next to the name of the user, then click **OK**.

Properties for the user display on the form.

6. Click **Submit Order**.

Adding or Removing an Organization Technical Administrator

This module explains how to change an existing user's role to Organization Technical Administrator (OTA) for an organization, or remove the user's Organization Technical Administrator role without deleting the user.

Note: If directory authorization has been enabled for your Cloud environment, then you may have to create users and assign, change, or remove roles from the directory rather than by using the Prime Service Catalog services outlined in this section. Directory integration can be configured so that users must be managed from the directory. In this case, any changes you make to an user using Prime Service Catalog will be overwritten by the definitions set in the directory.

Adding an Existing User as an Organization Technical Administrator

If directory authorization has been enabled for your Cloud environment, then you may have to create users and assign, change, or remove roles from the directory rather than by using the Prime Service Catalog services outlined in this section.

Directory integration can be configured so that users must be managed from the directory. In this case, any changes you make to an user using Prime Service Catalog will be overwritten by the definitions set in the directory.

1. Choose **Management > Tenant Management**.
2. On the Tenant Management page, choose the Users tab.
3. Next to the user you want to change, click the **gear** icon .
4. Choose Modify User Properties.
5. In the Assign Roles area, choose the radio button next to Organization Technical Administrator .
6. Update any other properties you would like to change.
7. Enter the First Name or Last Name of the user, or enter a wildcard *, and click **Search** to find the user.
8. In the Search Results area, click the radio button next to the name of the user you want to add as an Organization Technical Administrator, then click **OK**.
9. Click **Submit Order** and close the window that appears next when you are done reviewing it.

Creating a New User to Add as an Organization Technical Administrator

If directory authorization has been enabled for your Cloud environment, you may have to create users and assign, change, or remove roles from the directory rather than by using the Prime Service Catalog services outlined in this section. Directory integration can be configured so that users must be managed from the directory. In this case, any changes you make to an user using Prime Service Catalog will be overwritten by the definitions set in the directory.

1. Choose **Management > Tenant Management**.
2. On the Tenant Management page, choose the Users tab.
3. Click the **Add User+** button.
4. On the Add User page, choose Create New User from the drop-down list.
5. The page will repopulate for you to provide the following information:
 - Enter the first and last name of the new Organization Technical Administrator.
 - Enter a unique login identifier for the new Organization Technical Administrator.
 - Enter the new Organization Technical Administrator's e-mail address.
 - From the drop-down list, choose the time zone associated with the new Organization Technical Administrator's primary address.
 - Enter and then re-enter the password for the new Organization Technical Administrator.
6. Click **Submit Order**.

Removing an Organizational Technical Administrator

Remove the Organization Technical Administrator (OTA) from a user without deleting the user. When a user's role is removed, the user becomes "role-less" and Status is automatically changed to Inactive. Inactive users can log in to Prime Service Catalog but cannot use any of its services. If you assign the user another role, you must change the user's status back to Active. See [Changing a User's Status to Active or Inactive, page 71](#).

1. Choose **Management > Tenant Management**.
2. On the Tenant Management portal, click **Remove Organization Technical Administrator** to open the form.
3. On the Remove Organization Technical Administrator form, click **Choose** to open the Choose Person dialog box.
4. Enter the First Name or Last Name of the user, or enter a wildcard *, and click **Search** to find the user.
5. In the Search Results area, click the radio button next to the name of the user you want to remove as an Organization Technical Administrator, then click **OK**.

Properties for the user display on the form.

6. Click **Submit Order**.

Managing Organizations and Users With Directory Integration

If directory service is enabled for your environment, you must add, modify, or remove users (Cloud Provider Technical Administrators, Organization Technical Administrators, and Server Owners) from the directory rather than using the Prime Service Catalog services described in this section. For instructions, see the documentation that came with your directory software.

Managing User Roles

By assigning a role to a user, you are granting a pre-defined set of permissions and access levels, depending on their purpose. For example, while a Server Owner manages individual servers within an organization, a cloud provider technical administrator oversees cloud system operations that support multiple organizations.

Adding or Removing a Server Owner

This section explains how to Assign a Virtual Server Owner or Virtual and Physical Server Owner role to a new or existing user. If directory authorization has been enabled for your Cloud environment, then you may have to create users and assign, change, or remove roles from the directory rather than by using the Prime Service Catalog services outlined in this section. Directory integration can be configured so that users must be managed from the directory. In this case, any changes you make to an user using Prime Service Catalog will be overwritten by the definitions set in the directory.

Note: An OTA can assign another OTA to the same organization.

Adding an Existing User as a Server Owner

Note: This is a one-to-one relationship

1. Choose **Management > Tenant Management**.
2. On the Tenant Management page, click the **Users** tab.
3. Click the **Add User** button at the top of the portlet to open the form.
4. On the Add User form, choose the organization to which you want to add the user from the Organization drop-down list.

Note: You can also do this same process using the Add User form, and choose “existing user” from drop-down.

5. Choose **Choose Existing User** from the Action drop-down list to display the Choose User field.

Note: If the user belongs to a different home organization than the organization you chose in Step 3, an alert will appear advising you that if you proceed, the user’s home organization will change to the organization you have chosen. If this is acceptable, click **OK**.

6. Click **Choose** to open the Choose Person dialog box.
7. In the Choose User field, click **Choose** to open the Choose Person dialog box.
8. Enter the First Name or Last Name of the user, or enter a wildcard *, and click **Search**.
9. In the Search Results area, click the radio button next to the name of the user, then click **OK**. Properties for the user display on the form.
10. Click **Submit Order**.

Creating an Organization Technical Administrator to Add as a Server Owner

1. Choose **Management > Tenant Management**.
2. On the Tenant Manager portal page, choose the tenant/organization.
3. Click to open the **Users** tab.
4. Click the **Add User** button at the top of the view to open the form.
5. On the Add User to the Tenant form, choose the organization to which you want to add the user from the Organization drop-down list.
6. Choose **Create New User** from the Action drop-down list.
 - Enter the first and last name of the new user as well as a unique login identifier for the user.
 - Enter the user’s e-mail address.
 - From the drop-down list, choose the time zone associated with the user’s primary address.
 - Choose the Organization Technical Administrator role.
 - Choose the time zone.
 - Enter and then re-enter the password for the user.
7. Click **Submit Order**.

Removing a Server Owner

Remove the Virtual or Virtual and Physical Server Owner role from a user, without deleting the user. When a user’s role is removed, the user’s account status is automatically changed to Inactive, and the user becomes “role-less”. Inactive users can log in to Prime Service Catalog but cannot use any of its services. If you assign the user another role, you must change the user’s status back to Active.

1. Choose **Management > Tenant Management**.
2. On the Tenant Manager portal page, choose the tenant/organization.
3. Click to open the **Users** tab.
4. Next to the user you want to modify, click the **gear** icon .

Changing the nsAPI User Account Username and Password

5. Click **Deactivate User** in the popover to open the form.
6. On the Deactivate User form, click **Choose** to open the Choose Person dialog box.
7. Enter the First Name or Last Name of the user, or enter a wildcard *, and click **Search** to find the user.
8. In the Search Results area, click the radio button next to the name of the user you want to remove as a Virtual Server Owner, then click **OK**. Properties for the user display on the form.
9. Click **Submit Order**.

Reassigning a Server Owner to Another Role

Change a user's Virtual Server Owner role to the Virtual and Physical Server Owner role, or vice versa.

Note: The other server role must be in same organization. In addition, note that when a user's role is removed, the user becomes "roleless," and is automatically given Inactive status. You must change the user's status back to Active.

1. Choose **Management > Tenant Management**.
2. On the Tenant Manager portal page, choose the tenant/organization.
3. Click to open the **Users** tab.
4. Next to the user you want to modify, click the **gear** icon .
5. Click **Modify User Properties** in the popover to open the form.
6. On the Modify User Properties form, choose the user's organization from the **Organization** drop-down menu.
7. In the Choose User field, click **Choose** to open the Choose Person dialog box.

The user's current home organization and role appear.

8. *Optional.* Update the user's first name, last name, or e-mail address.
9. For Assigned Role, change the user's Server Owner role by clicking the **Virtual Server Owner** radio button.
10. Click **Submit Order**.

Changing the nsAPI User Account Username and Password

During Prime Service Catalog setup, a local nsAPI user was created exclusively for use when configuring Prime Service Catalog API. You can change the username, password, or both.

Changing the nsAPI User Credentials in Prime Service Catalog

For information on how the nsAPI User was created, see the [Cisco Intelligent Automation for Cloud 4.2 Configuration Guide](#).

1. Choose **Organization Designer** from the module drop-down list, then click the **People** tab.
2. In the People pane on the left, enter **nsapi** in the search field, then click **Search**.
3. Click the **nsAPI username** to display user information.
4. Edit the values in either or both the username (Login) and password.
5. Click **Update**.

Updating nsAPI agents

When you change the nsAPI username, password or both, you must also reset all NSAPI Agent Properties using the “Set Agent Configuration” service.

Managing Server Load Balancing

Use the load balancing features of Cisco Intelligent Automation for Cloud 4.1 to monitor load balancing on your servers.

1. Choose **My Cloud > My Servers**.
2. Choose the **gear** icon  next to the server for which you want to check load balancing.
3. Investigate load balancing information.
4. Close window.

Managing Load Balancing on VDCs

1. Choose **My Cloud > My VDCs**.
2. Choose Manage Load Balancer.
3. Choose an organization.
4. Click **Submit**.

The Manage Load Balancers page displays.

5. Make adjustments as needed to:
 - a. Create,
 - b. Remove,
 - c. Create Virtual IP, and/or
 - d. Use Existing Virtual IP.
6. Click **Submit Order**.

Working With Cloud Services Routers

In Cisco Intelligent Automation for Cloud 4.1, the upper-limit of user networks per Organization has increased. The default upper limit for user networks is 64.

Note: An alarm is triggered when the 64 user networks limit is exceeded.

Because VMware supports a maximum of ten Virtual Network Interface Cards (vNICs) per Virtual Machine (VM), and since an Organization can have only one Cloud Service Router, each organization has a built-in limit of six user networks. Cisco IAC has overcome this limitation by creating the sub-interfaces on top of a single interface.

Note: Organizations can order Virtual Data Centers (VDCs) or add network to VDCs until the supported maximum networks by Network POD.

Implementation

- Continue using Interface 1, 2, 3, 4 for management, Internet, Enterprise, and Load balancer
- Create Interface 5 when VDC or add network to VDC is ordered.
- Create port profile in Nexus 1K and configure it for VLAN trunk mode.
- Add vNIC to CSR and attach the vNIC to the created port-profile.
- Add VLAN to port profile to which interface 5 is attached and create sub interface to the interface 5 for each network created.



Managing Templates

Managing Operating System Templates

Use the instructions in this section to manage your operating system templates.

Registering an Operating System Template

For information about registering operating system templates, see [Registering an Operating System Template, page 82](#).

Maintaining an Operating System Template

The Cloud Provider Technical Administrator can change the state of an operating system template to Maintenance to keep the template ready, but not be used for new servers within the Cisco IAC system. The template must be in Registered state to set it to Maintenance. To set the operating system template to Maintenance when already Registered:

1. Choose **Setup > Manage Infrastructure**.
2. Choose a **Platform Element** (such as VMware vCloud Director, OpenStack, Puppet, Cisco UCS Director and so on) to see that platform element's available list.
3. Click the **Templates** icon.
4. Using the **gear** icon  popup, choose **Cloud Resource Maintenance** for the line item you wish to set to Maintenance mode.
5. Close the popup when you are done.
6. Enter Price, Appcode (*optional*), Multi-tenancy field values and Tenants field values.
7. Click **Submit Order**.

Ignoring an Operating System Template

The Cloud Provider Technical Administrator can change the state of an operating system template to Ignored to administratively ignore a template. The template may be in Discovered, Registered, or Maintenance states to set it to Ignored. If the record was previously in Registered or Maintenance states, metadata on that record will be saved. To set the operating system template to Ignored:

1. Choose **Setup > Manage Infrastructure**.
2. Choose a **Platform Element** (such as VMware vCloudDirector, OpenStack, Puppet, Cisco UCS Director and so on) to see that platform element's available list.
3. Click the **Templates** icon.
4. Using the **gear** icon , choose **Ignore Cloud Infrastructure** for the line item you wish to set to Maintenance mode.
5. Close the popup when you are done.

Managing Server Templates

Cisco IAC provides the following types of server templates that users can choose when they order servers.

- Virtual machine (VM) template
- Operating system
- vApp template
- UCS service profile template

All three types of server templates are discovered and registered using the CloudSync Infrastructure Discovery portal. After registering, the template is then uniformly available to all users.

Registering a Virtual Machine Template

The Cloud Provider Technical Administrator (CPTA) can register an existing VM template in the cloud system for users to choose when ordering virtual machines. The template may be in Discovered, Maintenance, or Ignored states to be changed to Registered. Before you can register a VM template, it must first be defined in vCenter and discovered using the CloudSync Infrastructure Discovery portal.

1. Choose **Service Portal** from the module drop-down list and then click **Manage Cloud Infrastructure**.
2. Click the **VM Templates** icon.
3. Choose the line item you wish to register in the grid, then choose the **Register** button.
4. In **Register VM Template**, choose the **Operating System Family**, then the **Operating System**.
5. Enter a friendly name in **Display Name** and a **Description**.
6. Enter Price, Appcode (*optional*) and access Tenants field values
7. Click **Submit Order**.

Registering an Operating System Template

The Cloud Provider Technical Administrator (CPTA) can register an existing operating system template in the cloud system for users to choose when ordering servers. The template may be in Discovered, Maintenance, or Ignored states to change it to Registered.

Note: Before you can register an operating system template, it must first be defined on the CSP server and discovered using the CloudSync Infrastructure Discovery portal.

1. Choose **Setup > Manage Infrastructure**.
2. Click **OS Templates**.
3. Choose the line item you wish to register in the grid.
4. Click **Register**.
5. In Register Operating System Template, choose the Operating System.
6. Enter a friendly name in Display Name and a description in Description.
7. Enter Price, Appcode (*optional*) and access Tenants field values.
8. Click **Submit Order**.

Register a vApp Templates for vCloud Director

The Cloud Provider Technical Administrator (CPTA) can register a vApp template.

1. Choose **Setup > Manage Infrastructure**.
2. Click **vApp Templates**.
3. Choose the line item you wish to register in the grid.
4. Click **Register**.
5. In Register vApp Template, choose the vApp Template.
6. Enter a friendly name in Display Name and a description in Description.
7. Enter Price, Appcode (*optional*) and access Tenants field values.
8. Click **Submit Order**.

Registering a UCS Service Profile Template

The Cloud Provider Technical Administrator (CPTA) can Register an existing UCS service profile template in the cloud system for users to choose when ordering servers. The template may be in Discovered, Maintenance, or Ignored states to change it to Registered. Before you can register a UCS Service Profile Template, it must first be defined on the UCS Manager and discovered using the CloudSync Infrastructure Discovery portal.

1. Choose **Setup > Manage Infrastructure**.
2. Click the **Service Profile Templates** icon.
3. Choose the line item you wish to register in the grid, and click **Register**.
4. In Register Operating System Template, choose whether this is a Hypervisor Template. If yes, choose the vCenter Cluster.
5. Enter a friendly name in Display Name and Description.
6. Enter Price, Appcode (*optional*) and access Tenants field values.
7. Click **Submit Order**.

Ignoring a UCS Service Profile Template

The Cloud Provider Technical Administrator can change the state of a UCS service profile template to Ignored to administratively ignore a template. The template may be in Discovered, Registered, or Maintenance states to set it to Ignored. If the record was previously in Registered or Maintenance states, metadata on that record will be saved.

1. Choose **Setup > Manage Infrastructure**.
2. Click the **Service Profile Templates** icon.
3. Choose the line item you wish to set to Ignored in the grid, and choose **Ignore Cloud Infrastructure**.
4. Review the information to confirm that the chosen operating system template is the one that you want to remove, then click **Submit Order**.

Registering Puppet Role

Register the Roles you want to be made available to users ordering servers with configuration management. You need to follow the practice of using roles and profiles to work with Application Configuration Manager (ACM).

1. Choose **Setup > Manage Infrastructure**.
2. Click the **Service Profile Templates** icon.
3. Choose the line item you wish to set to Ignored in the grid, and choose **Ignore Cloud Infrastructure**.
4. Review the information to confirm that the chosen operating system template is the one that you want to remove, then click **Submit Order**.
5. Click the **gear** icon  next to the role.

Registering Chef Role

Register the Roles you want to be made available to users ordering servers with configuration management. ACM uses Chef roles for server configuration.

Managing Email Templates

Use the instructions in this section to manage your email templates.

Configuring Email Notification Templates

Cisco IAC includes a set of default (delivered as part of Prime Service Catalog) email notification templates that you customize for an organization. The cloud system sends the email notifications in response to events such as orders and system errors. Before users can start ordering cloud services, you **must** configure the email notification templates with the relevant sender and recipient addresses.

1. Choose **Setup > System Settings**.
2. On the Setup portal, click the System Settings tab.
3. Click **Modify Email Templates**.
4. On the Request Center tab in the Email Templates panel, update the following templates (the others are programmed using a service):
 - Ad-Hoc Task Started
 - Default Late Activity
 - My Services Departmental Reviews
 - My Services Financial and Departmental Authorizations
 - My Services Service Group Authorizations
 - My Services Service Group Reviews
 - Process Escalation
 - Service Link Error on External Task

Note: Use the page controls at the bottom of the Request Center tab to find each template you want to configure. In addition to the default templates listed above, you may modify any of the templates listed on either the Request Center or the Demand Center tabs.

5. In the General pane, modify any or all of the following attributes:
 - a. Enter the name of the template.
 - b. Enter the subject of the notification.
 - c. Enter a valid address to use as the sender.
 - d. Enter one or more valid recipient email addresses. For multiple recipients, separate email addresses using semicolons.

Note: You can use namespace variables in this field. For information on using namespaces, see the [Cisco Service Portal 9.1 Namespace Users Guide](#).

- Leave the Language field as is.

Note: In the current release of Cisco IAC, only “US English” is supported; any language choice you make will be ignored.

- Leave the **Request Center** radio button chosen by the Type field.

6. For the editing window, click one of the following radio buttons to choose an editor.
 - HTML Part
 - Text Part
7. In the editing panel, modify the default content and add optional content as needed.
8. Click **Update**.
9. Repeat STEPS 3 through 7 above for the email templates on the Request Center tab.

Assigning From Address for Email Templates

In addition to configuring the templates, you must also assign the From address for the default templates to use for outgoing notification email messages. Email addresses must be properly formatted (name@email.ext).

1. Choose **Setup > System Settings > System Settings** tab.
2. Click **Set System Email Account**.
3. Enter the email address you would like to use as the default from address for outgoing notification email messages in the **Sender Email Address** field.
4. Click **Submit Order**.

Assigning Mail Addresses for Queue Notifications

You must update the queue configuration settings with email addresses that will receive email notifications for changes in service queues. A queue is a repository for administrative tasks that need to be performed, such as monitoring service delivery, lease instances, and failed service remediation. Tasks are automatically added to the queue by the Cloud system. Users with permissions can see the queues, assign tasks, and take action on the tasks in Service Manager.

Cisco IAC ships with the following pre-configured queues:

- Default Service Delivery—Tasks that are currently unassigned.
- Cloud Service Cancellation—Tasks related to services that have been canceled.

- Cloud Service Delivery Management—Tasks related to services that fail after they are first ordered, and resubmission of failed services after they are remediated.
- Cloud Service Lease Administration—Tasks related to server leases.
- Cloud Service Remediation—Tasks related to services that failed and need remediation action.
- Cloud Service Approval Administration - Tasks that are waiting for an approval.

Cloud Provider Technical Administrators and Organization Technical Administrator monitor, assign, or address tasks added to the queues. Those users with access to the queues can perform the tasks added the queues. When a task is added to a queue or is assigned or reassigned to a user, the designated users receive email notifications. For information about working with queues, see the [Cisco Intelligent Automation for Cloud User Guide](#).

To prepare the queues for use, you must specify the email addresses of the users who receive email notifications when a task is added to a queue. If you skip this task, no one will receive notifications of changes to the queues.

Note: Remember to use mailing lists (aliases), not specific user email addresses. Also, be sure to configure email addresses for each queue.

1. Log in to Cisco IAC as a Site Administrator.
2. Choose **Organization Designer** from the module drop-down list,.
3. Click the **Queues** tab.
4. In the Queues pane, click **Default Service Delivery**.
5. From the menu on the right side of the window, click **Contact** to display the Contact pane.

Before configuration, the Contacts panel lists one test email address (typically, CloudServiceRemediation@domain.com).

6. Click within the **Value** field and edit the email address.
7. Choose **Email** from the **Type** drop-down.
8. Click **Update**.
9. Repeat STEPS 1 through 8, above, to add additional email addresses to the queue.
10. Repeat STEPS 4 through 8, above, for the remaining queues.

Modifying Email Notification Templates

Cisco Intelligent Automation for Cloud 4.2 (Cisco IAC) includes a set of default email notification templates that you customize for an organization. The cloud system sends the email notifications in response to events such as orders and system errors. The email templates must be customized with the sender and recipient addresses. You can also optionally customize the subject and message.

To modify the default email notification templates, perform the following steps.

1. Choose **Setup > System Settings > System Settings** tab.
2. Click **Modify Email Templates**.
3. On the Request Center tab in the Email Templates panel, click **Add Role Completion Notification** in the list.

4. In the General pane, modify any or all of the following attributes:

Field	Action
Name	Enter the name of the template.
Subject	Enter the subject of the notification.
From	Enter a valid address to use as the sender.
To(s)	<p>Enter one or more valid recipient email addresses. For multiple recipients, separate email addresses using semi-colons.</p> <p>Note: You can use namespace variables in this field. For information on using namespaces, see the Cisco Service Portal Namespace Users Guide.</p> <p>Note: If this field is not set, these email templates will not be sent. The requisition history might say they did, but the email will not be sent if an SMTP formatted email address is not entered. The email must be properly formatted (email@domain.com).</p>
Language	Leave as is. In the current release, only US English is supported; any language selection you make will be ignored.
Type	Click the Request Center radio button.

5. For the editing window, click one of the following radio buttons to choose an editor.

- HTML Part
- Text Part

6. In the editing panel, modify default content and add optional content as needed.

7. Click **Update**.

8. Repeat Steps 3 - 7, above, for the email templates on the Request Center tab.

For a complete list of the email templates, see the Email Notification Template Modification Checklist in the [Cisco Intelligent Automation for Cloud Configuration Guide](#).



Ordering Cloud Services

This module provides information and steps for ordering services. You have two portals from which you can order services:

- Service Portal > My Cloud > Order Services
- Service Catalog > Server and Data Center Services

Commissioning a Virtual Machine from Template and Installing an OS

Note: For more information on templates in Cisco IAC 4.1, see [Managing Templates, page 81](#)

1. Choose **My Cloud > Order Services**.
2. Click **Order a Virtual Machine from Template**.
3. On the Order a Virtual Machine form, choose the **VDC Name** to deploy the server into. Your choice populates the display only fields such as:
 - a. Current Number of Virtual Servers Available
 - b. Current vCPUs Available
 - c. Current Storage Available (GB)
 - d. Current Memory Available (GB)
4. Enter a friendly name to identify the virtual machine.
5. Choose **Windows** or **Linux** as the Guest Operating System Family.
6. Choose the platform and version number of the operating system.
7. Choose the OS Template Friendly Name that you want to use to create the new virtual machine.

Note: The selections available in this drop-down depend on the operating system that you choose. Once chosen, the full name will populate in the Operating System Template field.
8. Choose a Virtual Machine Size from the drop-down list (Small, Medium, Large or Extra Large). Your selection populates the display-only fields vCPUs and vRAM (GB).

Note: The vCPU and vRAM values are set for each server size option and cannot be changed individually. To view the vCPUs and vRAM (GB) values for an option, choose the option from the drop-down list. The values automatically populate the display-only fields immediately under the drop-down list.
9. In the Deploy to Network field, choose a network whose static IP address will be assigned to the new virtual machine. Your selection populates display-only fields for Network Selection, Routing Prefix, Subnet Mask, Address, Broadcast Address, vCenter Network Path, and UCS Network Description.
10. *Optional.* Choose a Lease Term from the drop-down list. Your selection populates the display-only fields # of Days For Lease, Lease Expiration Date, and Storage Expiration Date. For more information server lease terms and expiration dates, see [Managing Server Leases, page 17](#).

11. Enter and then re-enter a password that you will need to configure the new server on fulfillment. The password must conform to company and domain policy or the provisioning may fail during configuration.
12. Click **Submit Order**.

Commissioning a Virtual Machine

1. Choose **My Cloud > Order Services**.
2. Click **Order a Virtual Machine**.
3. On the Order a Virtual Machine and Install an OS form, choose the **VDC Name** to deploy the server into. Your selection populates the display only fields such as:
 - Current Number of Virtual Servers Available
 - Current vCPUs Available
 - Current Storage Available (GB)
 - Current Memory Available (GB)
4. Enter a friendly name to identify the virtual machine.
5. Choose **Windows** or **Linux** as the Guest Operating System Family.
6. Choose the platform and version number of the operating system.
7. Choose the OpenStack Image template you wish to use for deploying the virtual machine from the list. (For OpenStack only.)
8. Choose a registered Flavor from the list to determine the size of the OpenStack virtual machine. (For OpenStack only.)
9. Choose a Security Group for the new virtual server instance from the chosen VDC. If not chosen, the default security group will be used.
10. In the Assign SSH Keypair field, provision a keypair for secure access to your new server. If a keypair already exists for your account, it will be associated with the new server.
11. Allocate Floating IP Address pool to automatically assign a public floating IP to the new server.
12. Choose a network from Deploy to Network whose static IP address will be assigned to the new virtual machine.
13. In the Quantity field, choose the number of servers to Order.
14. Choose a Lease Term: **1 month**, **3 months**, **6 months**, **9 months**, or **12 months**. Your selection populates the display-only fields # of Days For Lease, Lease Expiration Date, and Storage Expiration Date. For more information server lease terms and expiration dates, see [Managing Server Leases, page 17](#).
15. Enter and then re-enter a password that you will need to configure the new server on fulfillment. The password must conform to company and domain policy or the provisioning may fail during configuration.
16. Click **Submit Order**.

Decommissioning a Virtual Machine

This section contains instructions on how to power-off and permanently remove an existing virtual machine from the Cloud resource pool, and release all associated resources for re-use.

1. Choose **My Cloud > My Servers**.

2. On the My Servers portal, locate and click the name of the virtual machine that you want to decommission. Detailed information about the virtual machine and icons for performing actions appear in the Take Action panel.
3. Click the **Decommission** icon. The Decommission Virtual Machine form displays the computer name, full path, and operating system.
4. Check the **Yes** check box to confirm the decommission.
5. Click **Submit Order**.

Creating a Virtual Data Center

A virtual data center (VDC) can be used by server owners in an organization to provision virtual and physical servers. Virtual data centers live in a POD and has datastores, resource pools, and community networks as resources associated to them.

Note: Multiple virtual data centers can be ordered by an organization for server owners to provision servers in.

A virtual data center has an associated size that determines limits for the number of virtual servers, physical servers, vCPUs, CPU MHz, storage, and memory. Limits are enforced by comparing the sum of the number of provisioned virtual and physical servers and the vCPUs, memory, and storage for a server size against the limits defined for the virtual data center size.

A VMware resource pool is created for each virtual data center. This allows further control of resource utilization by defining CPU and memory limits, as well as CPU and memory reservations in the VMware resource pool.

Note: You must be either an Organization Technical Administrator (OTA), a Tenant Technical Administrator (TTA), or a Cloud Provider Technical Administrator (CPTA) to create a virtual data center. Create Virtual Data Center ordered by an OTA requires authorization by a CPTA.

Note: It is not possible to add a VDC if the datacenter does not have a cluster. Cisco IAC does not support data centers with 1 host (no cluster).

The following procedure shows an Organization Technical Administrator ordering a virtual data center. If the Cloud Provider Technical Administrator orders the Create a Virtual Data Center service, all the fields that are available during authorization moment will be visible during the ordering moment and the requisition will not wait for the authorization.

1. Choose **My Cloud > My VDCs**.
2. On the Create Virtual Data Center form, choose the Tenant Name.
3. Select the Organization Name.
4. Then specify the following information:

Field	Action
VDC Name	Enter a descriptive name for the virtual data center. This name will be displayed when the server owners choose the virtual data center.
Community VDC	Select Yes or No to set whether the VDC will be community shared or not. Note: To use existing networks with community VDC, the network must be marked as a community network.
Description	Enter a description for the virtual data center.

Field	Action
Size	Choose the size of the virtual data center. The size determines the maximum limits for the number of virtual servers, maximum number
Compute Pod	Choose the POD in which to place the virtual data center.
Choose a Network Service	Choose the type of network service from the drop-down list.
Number of Networks	Read-only
Radio button	<ul style="list-style-type: none"> ■ Provision New Networks ■ Choose from existing Networks
Number of Networks	A virtual data center can contain multiple networks. Choose the number of networks for this virtual data center. If more than one network is chosen, additional Add Network sections will be displayed on the form.
Max Hosts	Choose the number of hosts needed per network. This is used to determine the size of the network that will be assigned to the virtual data center.

5. Click **Submit Order**.

The requisition will go to the Cloud Provider Technical Administrator for approval.

Decommissioning a Virtual Data Center

You must be an Organization Technical Administrator (OTA) or a Cloud Provider Technical Administrator (CPTA) to perform this action. Note that all networks, virtual machines, and physical machines must be removed from the virtual data center prior to decommissioning.

1. Choose **My Cloud > My VDCs**.
2. On the My VDCs page, locate the virtual data center in the grid.
3. Click the **gear** icon .
4. In the popup, click **Decommission VDC**.

In the Decommission Virtual Data Center window, that follows the VDC Name field will be pre-populated with the chosen virtual data center name.

5. Click the radio button next to **Confirmation** to confirm action.
6. Click **Submit Order**.



Managing Tenants

Tenant in the context of a cloud infrastructure and SaaS is simply another name for “customer.” An organization would have many “customers,” or tenants, and its organization (and users) could be part of a shared infrastructure.

In Cisco Intelligent Automation for Cloud 4.2, no tenant can determine the existence of any other tenant; tenants may only see members of their own tenancy (users and groups/roles). Because tenants are authenticated and authorized to access their data, no tenant can access the data of any other tenant, including:

- Data in motion (network)
- Data at rest (storage)
- Data in memory (compute)

In addition, no tenant can perform an operation that might impact the service of another tenant outside of shared services. Each tenant’s configuration cannot be limited by any other tenant’s existence or configuration in any way, including by naming or addressing.

Note: Note that a given cloud provider may have some inherent access to the data within their own infrastructure. Cisco IAC supports an individual’s membership to a single organizational unit or membership (not multiple).

About the Tenant Management Form

Note: When you choose a tenant, all tabs are exposed. When chosen on an organization only the following tabs are exposed: Details, Service Offerings, Users, Run Rates, Service Group, and Server Groups.

The Tenant Management form offers access to the following tabs:

- **Details**, which includes data such as:
 - People
 - Template
 - Infrastructure
 - Run Rate
- **Service Offerings**, which displays a list of services available to this tenant or organization, depending what is chosen. Note that both chosen to unchosen options will be visible.
- **Users**, which includes:
 - Role
 - First Name
 - Last Name
 - User ID
 - Email

About the Tenant Management Form

- **Run Rates**, which includes:

- Total Run Rate
- Current Rate
- Service Name
- Type
- Date

- **Service Group**, which includes:

- Service Group Name
- Organization Name
- Firewalls
- Load Balancer

- **Server Groups**, which includes:

- Name
- Type
- Tenant

Available actions associated with a particular Server Group can be accessed using the popover.

- **Quotas**, which shows a graphical run rate-o-meter

- **Template Catalog**, which includes:

- Template Name
- Name
- Operating System
- Description

- **Pricing**, which includes:

- Rate Code
- Rate
- Unit Of Measure
- ACMRole
- CSPTemplate

- In addition, a Dashboard button displays the **Tenant Dashboard** showing you:

- Tenant Statistics
- Run Rate Quota (as a horizontal bar chart)
- Application Use

Onboarding a Tenant

- Run Rate Summary, and
- User Data by Role

Onboarding a Tenant

In Cisco Intelligent Automation for Cloud 4.0, you create tenants by onboarding them. Tenants are your customers who share the Cisco IAC environment. The framework provides the ability to bring new enterprises on board the existing configuration. This framework separates organizations from each interfering with each other. To onboard a new tenant:

1. Choose **Management > Tenant Management**.
2. On the Tenant Management screen, scroll down and click **Onboard Tenant**.
3. Enter the full name of the company, the company abbreviation (maximum 4 characters), and the (*optional*) description.
4. Choose the **Run rate limit** (used to determine the quotas for the tenant). Limits are:
 - Small
 - Medium
 - Large
 - Unlimited

Note: Run rate limit is ideal for the cautious Tenant, who in conversation with the CPBA, has yet to be comfortable with their spending in the cloud. Choose Quotas allows the Tenant (the TBA) to cap the cloud expenditure. This ability to create a cap may help make many Tenants more comfortable when signing up for cloud services.

5. Choose the **Currency**. Currencies include:

Table 1 Available Currencies (Alpha Sort, by Column)

Australian Dollars	Euro	Lempiras	Riels
Baharnae Dollar	European Currency Unit	Leva	Ringgits
Baht	Fiji Dollar	Liberia Dollars	Riyals
Balboa	Forint	Liras	Rubles
Barbados Dollar	Francs	Lire	Rupees
Belize Dollar	Guarani	Liri	Rupiahs
Bermuda Dollar	Guilders	Litai	Shillings
Bolivares	Guyana Dollars	Meticaiss	Singapore Dollars
Bolivianos	Hong Kong Dollars	Nairas	Solomon Islands Dollars
Brunei Darussalam Dollars	Hong Kong Dollars - BOC notes	Namibia Dollars	Soms
Canadian Dollars	Hong Kong Dollars - HSEIC notes	New Manats	Sums
Cayman Islands Dollar	Hong Kong Dollars - SCEI notes	New Shekels	Suriname Dollars
Cedis	Hryvnia	New Lei	Switzerland Francs
Colon	Jamaica Dollars	New Lira	Taiwan New Dollars

Table 1 Available Currencies (Alpha Sort, by Column)

Colones	Kips	Nuevos Soles	Tenge
Convertible Marka	Koruny	Pesetas	Trinidad and Tobago Dollars
Cordobas	Krone	Pesos	Tugriks
Cruzeiros	Kroner	Pounds	Tuvalu Dollars
Denars	Kronor	Pulas	United States Of America Dollars
Dinars	Kronur	Punt	Won
Dong	Krooni	Quetzales	Yen
Drachmae	Kuna	Rand	Yuan Renminbi
East Caribbean Dollar	Lati	Reais	Zimbabwe Dollars
EUR	Leke	Rials	Zlotych

6. Choose a Private Subnet.

Note: In the event that a Tenant chooses to have a Connectivity Type of “Enterprise” or “Internet,” this private subnet range should be non-overlapping with the Tenant’s existing Enterprise networks.

7. Choose a Primary Contact. At this point, you can now choose an existing user or create a new user.

- If you choose to **Create New User** as the Action.
 - Enter the first name and last name of the new user.
 - Type a unique login identifier.
 - Enter a Password and Confirm the Password.
 - Enter the contact e-mail address and contact title.
 - Enter the Primary Contact phone number.
 - Enter the physical (shipping/mailling) address (*optional*).

8. Set Tenant-wide Service Options.

Note: By default, services related to Virtual Security Gateways (VSGs), Cloud Services Routers (CSRs) and Adaptive Security Appliances (ASAs) are turned off. This is to comply with Cisco’s Multiple Security Zones, Enhanced VM Security, Load Balancing Services. If you need services related to VSGs, CSRs, and/or ASAs, you must manually enabled them as and when needed.

Options include:

- a. Virtual Machine From Template Ordering
- b. Application Configuration Management
- c. Service Assurance
- d. Virtual Data Center Ordering
- e. Physical Server Provisioning
- f. Install OS Ordering
- g. Community VDC Ordering
- h. Advanced Network Services

Offboarding a Tenant

- i. Multiple Security Zones
 - j. Mandatory for Advanced Network Services set to Yes
 - k. Enhanced VM Security
 - High Availability (visible only when Enhanced VM Security is set to Yes)
 - l. Load balancing Services
9. Choose a connection type for Virtual Data Centers for this tenant.
- a. Enter the Enterprise VRF Connection to be used as transit network for Enterprise Connectivity. VDC Connection Type has three options:
 - **Both:** Internet and Enterprise
 - **Internet:** Internet only
 - **Enterprise:** Enterprise only, which if chosen presents the user with options for Enterprise Transit Network, Enterprise Gateway, and Enterprise BGP Peer which will override the system defaults (Set Provision Settings)
- Note:** The choice of Connection Type and Service Offering Elections have a cascading affect on availability of connection types and services offering to underlying organization and its users.
10. Click **Submit**.

Offboarding a Tenant

1. Choose **Management > Tenant Management**.
2. On the Tenant Management page, scroll down and click Offboard Tenant.
3. On the Offboard Tenants form, review and complete all of the necessary information as pertains to this tenant.
4. Scroll down and click the **Confirmation: Yes** check box.

Caution: This action can lead to loss of data.

5. Scroll down further and click **Submit**.

Modifying a Tenant

1. Choose **Management > Tenant Management**.
2. On the Tenant Management page, scroll down and click Modify Tenant.
 - a. On the Modify Tenant form, modify the information as needed (all fields are optional):
 - b. Provider Name
 - c. Name of the company and/or the company description
 - d. Run rate limit
 - e. Modify/choose currency
 - f. Change service offerings (CPTA and CPBA only)
3. Make all other modifications as needed.

Viewing Tenant Information

Note: See [Onboarding a Tenant, page 95](#) for more detailed information about all of the fields on this form.

4. Click **Submit**.

Viewing Tenant Information

A Tenant Business Administrators (TBA) would use the information available here to quickly discern which organization is spending the most/least in the cloud. In addition, he or she can discern which cloud service is costing a given organization the most and the least.

1. Choose **Management > Tenant Management**.
2. Use the Dashboard (to the right of the screen) to view information, some in chart format.

Note: It can take a few minutes for the Dashboard to populate. You may think that the Dashboard has stopped working, but it hasn't. Continue to wait.

3. Hover over, and/or click on, an item to drill down or to see additional information.
4. Exit when done.

Understanding Multi-Tenancy Views in VMware and UCS Manager

VMware vCenter

The folder structure in vCenter in the VM and Templates view is such that provider troubleshooting is easier, tenant namespace is guaranteed, and CloudSync may consider tenancy.

UCS Manager

The folder structure for UCS Manager is such that provider troubleshooting is easier, tenant namespace is guaranteed, and CloudSync may consider tenancy.



Financial Management

The Cloud Provider Technical Administrator (CPBA) is in charge with overseeing and administrating a public or private cloud as a revenue generating business. This covers determining the mix of services that the public or private cloud is offering in the market as well as determining the pricing of services and service options.

In a multi-tenant cloud, the Tenant Business Administrator (TBA) is the commercial and business authority within the tenant and represent these concerns to the cloud provider. These responsibilities include negotiating pricing, service options, service levels and other service terms with the cloud provider and approving high cost service orders by tenant users.

Note: See [About the Tenant Management Form, page 93](#), which includes additional information on pricing as it relates to tenants.

Financial Management Features

Cisco Intelligent Automation for Cloud 4.2 provides the following financial management tools.

Pricing. A method to set pricing on common objects.

Showback. A mechanism to allow users to see the calculated cost of their potential orders during the ordering process.

Run Rates. Both a mechanism for users to see the recurring cost of the items that they own, as well as a mechanism for administrators to see the recurring cost of the items that their tenants own.

Billing Integration. Real-time billing events that can be consumed by a billing system within an extension point.

Note: Cisco IAC does *not* provide billing (such as invoicing and payment transacting) functionality, nor metering (financial management based on measured utilization) functionality.

Note: You have the ability to set one-time rate or recurring for Chef and Puppet during registration. After that, only recurring will show on Run rate (not one-time costs).

Pricing Models

Volumes and vApps

■ vApps

For vCloudDirector we have new rate table in 4.2 for vApp Containers that includes all the VMs underneath (within) the vApp container.

■ Openstack Volumes

For Cisco IAC 4.2 we are using VMStorage rate table for OpenStack Volumes: \$1.0/GB storage per billing cycle.

■ Physical Servers

For the physical server, we are using PSCPU and PSSStorage tables.

Complex Pricing

Cisco Intelligent Automation for Cloud supports complex pricing including:

- **Consumption-based Pricing.** This is pricing done on the individual, atomic units of cloud infrastructure.
- **Reservation-based Pricing.** This is pricing based on the assignment of cloud infrastructure to a tenant. Allocated infrastructure may or may not be reserved, which allows for over-subscription; for example, floating IP addresses or a small VDC.

Note: Whether the infrastructure that comprises a VDC is in fact reserved by the provider for use solely by the tenant is a choice left to the provider.

- **Both Consumption and Reservation-based Pricing.** For example, virtual machine with multiple disks attached.
- **Application-based Pricing.** Pricing by application.

Note: You set pricing for applications at the tenant level (**Management > Tenant Management**). See [Managing Tenants, page 93](#)

Billable Items

The following are the billable items available in Cisco Intelligent Automation for Cloud:

- **Virtual Data Centers.** VDC Package Size: Each size defaults to \$0 (configurable).
- **Network Appliances.** Cisco CSR 1000v, Cisco Prime NSC, Cisco VSG, and Citrix NetScaler 1000v.

Note: Each appliance is assigned a default price.

- **Networks**
- Applications
- **Floating IP Address and Virtual IP Addresses.** (Default price for FIPs is US\$3; for VIPs, US\$0).
- **Virtual Machines.** Server Size, Template (no default price), CPU, Memory (GB), Total Storage (GB).

Default Pricing

Default prices are provided to facilitate initial product deployment. You can also use default prices to:

- facilitate conversations with the customer
- provide a starting point for consideration of customization
- facilitate proof of concepts and product demonstrations

Note: Default prices should be replaced with deployment-specific pricing

Pricing for Physical and Virtual Servers Based on Server Templates

Server Templates are not shipped with Cisco IAC. However, Cisco IAC does include templates from many different cloud platforms. These templates do not have prices defined by default. You will need to define prices upon registration of the template.

Table 1 Server Templates

Server Type	Template	Price (units of currency)	Interval
Virtual	OS Template	Set upon registration	One-time
Virtual	vCenter Template	Set upon registration	One-time
Virtual	EC2 Image	Set upon registration	One-time
Virtual	OpenStack Image	Set upon registration	One-time

Pricing for Virtual Servers Based on Server Size

In Cisco IAC, “provisioned” Virtual Machines (VMs) are priced by assigned server size. There is a surcharge for any additional resources (such as additional CPUs). Upon registration, “discovered” VMs will have size “custom” assigned. No price is associated with the “custom” size.

Table 2 Server Pricing

Server Size	CPU	Mem (GB)	Storage (GB)	Price (units of currency)	Interval
Extra Small	1	1	30	21.50	Per Billing Cycle
Small	2	2	30	41.50	Per Billing Cycle
Medium	2	4	40	62.00	Per Billing Cycle
Large	4	6	40	102.00	Per Billing Cycle
Extra Large	8	8	60	163.00	Per Billing Cycle

Additional Resources

Table 3 Additional Server Resources

Infrastructure	Type	Unit of Measure	Price (units of currency)	Interval
CPU	Virtual	1	20.00	Per Billing Cycle
Memory	Virtual	1 GB	2.00	Per Billing Cycle
Storage	Virtual	1 GB	1.00	Per Billing Cycle

Pricing for Virtual Data Centers

Table 4 Default Resource Prices

VDC Size	Price (units of currency)	Interval
Small	0	Per Billing Cycle
Medium	0	Per Billing Cycle
Large	0	Per Billing Cycle

Pricing for Network Services

Table 5 Default Resource Prices

Network Resources	Price (units of currency)	Interval
Cisco CSR 1000v	30	Per Billing Cycle
Cisco VSG	20	Per Billing Cycle
Citrix NetScaler 1000v	30	Per Billing Cycle

Pricing Example

CSR 1000v (L-CSR-50M-STD-1Y=)

- 1-year license for 50 Mbps Max throughput, Standard package, excludes SASU3, 4GB RAM, 4 CPU
- This is a one year license with 50Mbps throughput at \$350, so we're looking at monthly pricing of $\$350/12 = \29.16

Pricing for Applications

The table below is for example purposes only. Applications and prices are not provided out of the box with Cisco IAC 4.2.

Table 6 Default Application Prices

Application	Price (units of currency)	Interval
mySQL	0.00	Per Billing Cycle
Apache	0.00	Per Billing Cycle
PHP	0.00	Per Billing Cycle
msSQL	55.00	Per Billing Cycle
Oracle 11G Enterprise	3000.00	One-time Billing
AutoDesk Desktop	39.00	Per Billing Cycle
Puppet Enterprise	29.00	Per Billing Cycle

As a CPTA, pricing can be defined and tracked per application basis. The CPTA will need to modify the default prices according to each application. Each application can be defined based on the run rate and pricing per the billing cycle.

Note: OpenSource applications usually do not have a price associated to the application. Therefore, Opensource applications should be set to '0.00'.

Pricing for Floating and Virtual IP Addresses

Table 7 Floating and Virtual IP Addresses

IP	Price (units of currency)	Notes
Floating IP	3	Based on consumption of a public IP address.
Virtual IP	0	Based on consumption of load-balancing services.

Financial Management by Persona

Operations Performed by Cloud Provider Business Administrators

Cloud Provider Business Administrators perform any or all of the following operations:

- View all tenants' run rates
- View a single tenant's run rates
- Set system-wide prices
- Modify prices per tenant

Setting Prices on Cloud Services

Setting Prices For All or Specific Tenants

For Server Templates. Upon registration of the template, price will be set for all tenants who are given access to the template. To preserve historical pricing, upon update of the template, price will not be changed for existing users (tenants) of the template, but only for tenants who are given new access to the template.

For All Other Cloud Resources. Go to **Price Rates**. Update the price rate tables for all or specific tenants.

Note: Bulk operations are not supported, but grandfathering of all pricing is supported.

Setting Different Prices For Different Tenants

System-Wide Pricing. A "Master Rate Group" defines system-wide pricing and shipped with the product. Default prices facilitate the ability to quickly deploy the solution as well as product demonstrations.

Tenant-Specific Pricing. A tenant-specific rate group is created when each tenant is onboarded. New tenants receive default pricing set by the provider in the "Master Rate Table". Tenant-specific pricing may be configured once the tenant has been on-boarded.

Note: Default prices should be replaced with deployment-specific pricing.

Setting Price Rates

You can set, modify, and delete price rates per tenant using the Price Rates feature.

1. Choose **Service Portal > Price Rates**.

Setting Price Rates

The Billing Rates page displays. The purpose of this page is to allow the CPBA to define standard prices for cloud services offered, as well as to define tenant-specific rates. For example, the CPBA could give a particularly good customer a special discount rate.

2. Manage price rates as needed. You can switch between tabs as you work: Billing Rate Definition and Billing Rate Table.
3. On the Billing Rate Definition tab, complete the following:
 - a. Display Name
 - b. Name
 - c. Service Item Type
 - d. Rate Group
 - e. Description
4. In the Billing Rate Attributes area, choose whether the following are for Billing or are Memo Fields.
 - a. Name
 - b. ServerServiceItemtype
 - c. Serverserviceitemhdarne
 - d. ACMServiceItemtype
 - e. ACMServiceItemName
 - f. ACMServerType
 - g. Billable
 - h. ACMRme
5. In the Billing Rate Operations area, indicate which operations should be applied, such as OrderRole.
6. Choose the Billing Rate Table tab to access the billing rate table area.
7. Edit the billing rates for the various related fields. You can add or edit the information in the following fields:
 - a. Rate Code
 - b. Rate
 - c. Unit of Measure
 - d. ACMRole
8. Use the **Add+** button to add new Rate Tables and Rate Groups.
9. When done, close this portlet.
10. Click **Save** when you are finished.

Note: We strongly advise you to NOT change the Rate of Measure on this window. Doing so will cause the UI showback calculation to stop working. There is a “Master Rate Group” controlling default prices system-wide for all newly-onboarded tenants.



Provisioning and Managing Networks

Cisco IAC 4.2 allows you to add, remove, and modify networks. This module explains the processes involved in managing your networks. You can define a network using VMware vCenter port groups as well as auto-provision a network by creating new VMware vCenter port groups.

Network Types

Add an L2/L3 network for cloud system use, for a community VDC, or for a virtual data center. You can add the following types of networks:

User Networks

Define a shared or controlled-access network within the cloud system for users in an organization to deploy servers.

Community Networks

Community networks provide the same purpose as a user network, but are available to any cloud user for deploying servers.

Management Networks

A management network can optionally be assigned to a user network. A management network within the cloud system may be used to manage cloud servers; for example, for remote access and monitoring. When a management network is assigned to a user network and a server is deployed with two network interfaces, the first network interface will be placed into the user network and the second network interface will be placed into the assigned management network.

Infrastructure Networks

Infrastructure networks are used to deploy the management interfaces of the components which make up your cloud. Generally this represents the management network for VMware ESX hosts. Registration of at least one infrastructure network is required for automated provisioning of ESXi hosts. Infrastructure networks may also be used as Service Networks and Internet Transit networks in the Service Resource Container used in Virtual Network Services deployments. In addition, for the Management of Advanced Network Services Virtual Devices when Organizations are deployed.

Adding an Existing Network

1. Choose **Setup > System Settings > Networks** tab.
2. Choose Add a Network.
3. On the Add a Network form, specify the following:
 - a. Enter a short network name that will be shown to users in the drop-down lists.
 - b. Enter the network for this subnet in CIDR notation. Enter only an IPv4 type of IP address. For example, 192.168.1.x/24.

Note: Subnets from /23 to /29 are supported.

Adding an Existing Network

- a. Choose the network access scope for user networks. A community network is available to users in shared zones. Non-community networks require explicit VDC level access to be set before users can deploy servers to it, which can be useful for traffic isolation and better security.
 - b. Specify Public or Private; for Public select **Yes**. Public networks are globally unique; private networks must only be unique within associated network device contexts.
 - c. Choose Network Type, such as **User**.
 - d. Choose how IP addresses management is done in this network: Internally by Cisco IAC, or via an external IP management tool.
4. Choose the port profile corresponding to the IP range being created.
- a. Choose the UCS VLAN that corresponds to the IP range being created. The UCS VLAN should match the VLAN for the port profile.
 - b. *Display only*. The subnet mask is generated from the prefix of the vCenter network you specified on this form.
 - c. The “gateway” address is the floating “VIP” shared by the real members.
 - d. Use the default gateway network that is populated from the subnet address or enter a different gateway network address (for example, 192.168.1.x).

The pre-population of the gateway address is a convenience feature; if it does not suggest the address that is right for your network, you should either correct or remove it. This IP address will not be assigned to any server deployed by the system.

5. FHRP is a term used to describe the various First Hop Redundancy Protocols. This includes HSRP (common at Cisco) and VRRP (common outside of Cisco). The FHRP 1 and 2 address are the “real” IP addresses of the routers participating in the redundancy protocol.
- a. Enter the FHRP (First Hop Redundancy Protocol) gateway 1 and 2 network IP addresses, or keep the default values.

The pre-population of the FHRP addresses are a convenience feature; if they do not suggest the address that is right for your network, you should either correct or remove them. These IP addresses will not be assigned to any server deployed by the system.

- b. Use the default broadcast address that is populated from the subnet address or enter a different broadcast network address. For example, 192.0.2.255. This IP address will not be assigned to any server deployed by the system.

Enter one of the following:

- The valid primary DNS address for servers on this network
 - A dummy primary DNS address.
- c. This IP address will not be assigned to any server deployed by the system. Enter one of these:
- The valid secondary DNS address for servers on this network.
 - A dummy secondary DNS address.

Note: Amazon reserves the first four (4) IP addresses and the last one (1) IP address of every subnet for IP networking purposes. In Amazon networks, IP addresses should be marked as *excluded* using the Network Management page.

6. Click **Submit Order**.

Removing a Network

You can remove a Layer 3 network, including its IP Pool, and disassociate it from port profiles. When you remove a network, the process first disassociates the IP addresses from the chosen network, and then removes the network mapping of this network.

1. Choose **Setup > System Settings > Networks** tab.
2. Click Remove a Network.
3. On the Remove Network form, choose the Network Name.
4. Click **Submit Order**.

Managing Network IPs

To view a list of your networks and IP capacity information for each network:

1. Choose **Operations > Network Management**.
2. Explore the dashboard as needed.

Managing IP Address Exclusions

You will want to manage exclusions to facilitate Brownfielding existing networks, which may have existing hosts. These hosts will have prior IP address assignments that need to be accounted for; these will need to be excluded from use. The Network Management page also allows the CPTA to manage individual network utilization.

1. Choose **Operations > Network Management**.
2. The Manage Networks form displays.
3. Choose the Network from the top table.
4. Use the IP Address Assignments table check box at the top of the table for bulk updates.
Note: For updating single IP address, check the check box next to of any IP Address .
5. When you are done, click **Save** to initiate the bulk update.

Adding a Public Subnet to a Network POD

You will want to add a Public Subnet to a Network POD to provide a collection of available, public IP addresses to be used for assignment to singular servers as either Floating or Virtual IP Addresses. The services are used by load-balancing and Network Address Translation (NAT) services. Individual IP address assignment are created as either a Floating IP Address (for NAT) or a Virtual IP Address (for load-balancing).

1. Choose **Setup > System Settings > Networks** tab.
2. Click Add Public Subnet to a Network POD.
3. On the Add a Public Subnet to a Network POD form, complete the required fields:
 - a. Subnet Address: The network address of the subnet
 - b. Subnet Bitmask: The bitmask (numeric) of the subnet you are adding. Do not include the slash.

Adding a Network to a Community VDC

- c. Assigned Subnets: The public subnets that have already been assigned.
 - d. Unassigned Subnets: The free public subnets remaining in the pool.
4. Click **Submit Order**.

Adding a Network to a Community VDC

After a community VDC is provisioned, additional networks can be added. Since community VDCs are a community virtual center, networks are added to the community VDC through the My Virtual Data Centers portal page. The network to be added must already exist. Only community networks can be added to the community VDC. To add a network to the community VDC:

1. Choose **My Cloud > My VDCs**.
2. Choose the community VDC in the list of virtual data centers that a network should be added to.
3. Click the **Add Network to VDC** action.
4. In the Network Name field, choose the network to be added. Only community networks are shown.
5. In the Management Network field, optionally choose a management network to be associated with the community network. The management network should be the same subnet size as the community network.

Provisioning a New Network for a Virtual Data Center

After a virtual data center is created, Organization Technical Administrators (OTAs) can request additional networks for the virtual data center. Once the request is submitted, the Cloud Provider Technical Administrator (CPTA) may need to approve the request and assign a new network to the virtual data center. The network to be added must already exist. If the Cloud Provider Technical Administrator initiates the request, he or she can directly assign a new network to the virtual data center and the request will not go for approval. To add a network to virtual data center:

1. Choose **My Cloud > My VDCs**.
2. Click Add Network to VDC.
3. Choose the number of hosts per network needed for the network to be added. This is used by the Cloud Provider Technical Administrator to determine which size network subnet to assign to the virtual data center.
4. Click **Submit Order**. The requisition will go to the Cloud Provider Technical Administrator for approval.

Defining a Network Using Existing Port Groups

Viewing the List of All Networks

To view a list of your networks and IP capacity information for each network:

1. Choose **Operations > Network Management**.

You will see a portal displaying your Networks and IP Address Assignments.

Obtaining Approvals for Adding a Network to a VDC

After an Add Network to VDC requisition is submitted by an Organization Technical Administrator, it goes to the CPTA's Cloud Service Approval Administrator queue for approval. The CPTA must assign a network to the virtual data center and then approve the requisition.

1. Choose **Operations > Approvals**.
2. Click on the **Order #** for the Add Network to VDC requisition that requires approval. This brings up the requisition.
3. In the Network Name field, choose the network to be added.
4. In the Management Network field, optionally choose a management network to be associated with the community network.
Note: The management network should be the same subnet size as the community network.
5. Click **Update** to update the requisition with the VDC resource assignment information.
6. Click **Approve** for the request.

Deleting a Network from the Cloud System

The Remove Network from VDC process should completely delete a network from the cloud system in a single step. VDC networks will be deprovisioned and all resources will be returned to their respective pools. However, you may find it necessary under some circumstance to use the following procedure.

Note: Before you permanently remove a network you must first remove any IP address assignments associated with the network.

1. Choose **Setup > System Settings > Networks** tab.
2. Click Remove a Network.
3. On the Remove Network form, choose the network from the drop-down list. If the network has IP addresses associated with it, an alert will inform you, and you cannot proceed with the deletion.
4. Click **Submit Order**.

Removing a Network from a Virtual Data Center

1. In Prime Service Catalog, locate the virtual data center in the grid, then click the name.
2. In the Manage Virtual Data Center collapsible panel, click on **Remove Network from VDC**.
3. Choose the network you want to remove from the **Network Name** drop-down list.
4. Click **Submit Order**.

Auto-Provisioning a Network Using New Port Profiles

If there are no existing port profiles, or if users have a need for new port profiles, Cisco IAC will auto-provision the port profiles with the creation of the networks—there is no need to run Add Network as a separate service. Also, any time you delete a network, Cisco IAC auto-deletes any port profiles created as part of an auto-provision (not any of the previously-created port profiles).

Note: The above applies to ANS on vCenter only.

A Note About Prerequisites

The following pools are required to be available in order to successfully auto-provision a network using new port profiles:

- **Private IP Address Pool** - This is set up during the Create Tenants process (onboarding tenants) (see [Onboarding a Tenant, page 95](#)).
- **VLAN Pool** - This is set up during the Create Network Pod process. Information on creating and managing PODs can be found in the [Managing PODs, page 127](#).



Managing Virtual Machines and Data Centers

Cisco Prime Service Catalog hosts the customer-facing element of Cisco IAC 4.2, where users log in and order services.

Viewing Server Status and Properties

The My Servers portal provides information about all of your active servers. You can monitor status, manage snapshots, verify that a server you that ordered has been delivered, and manage power, modify configuration, take snapshots, decommission, and extend an existing lease.

1. Choose **My Cloud > My Servers**.

The My Servers portal displays active servers in a table with information about each server, including operating system, organization, and server owner. Additional columns are available.

Note: To add columns to the table, and to re-sort the rows, see [Customizing Table Views, page 8](#).

2. To display more details about a server or take action (see list of actions below), click the **gear** icon next to the server name to display the popover. The actions are categorized in two sections on the popover:

Server Operations

- Power Up
- Power Down
- Power Cycle
- Modify Configuration
- Decommission Virtual Machine
- Modify Server Ownership
- OpenStack

Lifecycle Management

- View Snapshot
- Take Snapshot
- Revert to Snapshot
- Delete Snapshot
- Manage Applications
- Extend Server Lease

Note: If a server is in the process of being provisioned, all of the icons are disabled.

Powering Up a VM

To power up a server or VM and start the boot process, follow these steps:

1. Choose **My Cloud > My Servers**.
2. On the My Servers portal, locate and click the VM you want to power up.
3. Click the **gear** icon  next to that server.
4. In the popup panel, click the **Power Up** icon.

You will see a notice informing you that your request has been submitted.

5. Close the popup.

Powering Down a VM

To power down an active VM, regardless of its operating system state, follow these steps.

1. Choose **My Cloud > My Servers**.
2. On the My Servers portal, locate the VM you want to power down.
3. Click .
4. Click the **Power Down** icon in the popup.

You will see a notice informing you that your request has been submitted.

5. Close the popup.

Power-Cycling a VM

1. Choose **My Cloud > My Servers**.
2. On the My Servers portal, locate the VM you want to power cycle.
3. In the Manage panel, click the **Power Cycle** icon.

You will see a notice informing you that your request has been submitted.

4. Close the popup.

Changing the Server Size of a Virtual Machine

Change the vCPU and vRAM (GB) sizes of a virtual machine. To commission a virtual machine, see [Commissioning a Virtual Machine from Template and Installing an OS, page 89](#) and [Commissioning a Virtual Machine, page 90](#). The vCPU and vRAM values are set for each server size option and cannot be changed individually.

Note: Changing the server size of a virtual machine is an action available only to CPTAs, TTAs, and OTAs.

Available server size options are customizable by Administrators, and so may vary from the default options that ship with Cisco IAC. To view the vCPU and vRAM values for a server size option, choose the option from the drop-down list. The vCPU and vRAM values automatically populate the display-only fields below the drop-down list.

1. Choose **My Cloud > My Servers**.
2. On the My Servers portal, locate and click  next to the server you want to change.

Taking a Snapshot of a Virtual Machine

3. In the popup panel, click the **Modify Configuration** icon.
4. On the Modify Configuration form, choose a new size (Extra Large, Extra Small, Large, Medium, or Small) from the **Virtual Machine Size** drop-down list.
5. Optional make modifications to the disk by clicking the disk icon next to **Manage Disks**.
6. On the popup, click **Add** to add new disks, as well as change the name and disk size. (You can type in the size or use the slider).
7. Delete a disk as needed.
8. Click **OK** to close the Manage Disks popup window.
9. Back on the Modify Configuration form, click **Submit Order**.

Taking a Snapshot of a Virtual Machine

Create, name, and store an image of the state of a virtual machine.

1. Choose **My Cloud > My Servers**.
2. On the My Servers portal page, click the name of the virtual machine to display the Take Action panel.
3. Click the **Take Snapshot** icon to open the Take Snapshot form.
4. In the snapshot name field, enter a unique and descriptive name for the snapshot.
5. Enter a description of the snapshot.
6. Click **Submit Order**.

Reverting a Virtual Machine Settings to Snapshot

Revert a virtual machine to a previous state using the snapshot of your choice.

1. Choose **My Cloud > My Servers**.
2. On the My Servers portal page, click the name of the virtual machine to display the Take Action panel.
3. Click the **Revert Snapshot** icon to open the Revert to Snapshot form.
4. From the Snapshot name drop-down list, choose the snapshot to which you want to revert the chosen virtual machine.
5. Check the **Confirm This Action** check box if you are sure that you want to revert the virtual machine to the snapshot, then click **Submit Order**.

Viewing Snapshots

View the history of snapshots taken of virtual machines within an organization. From the list, you can view history and related services of a snapshot.

1. Choose **My Cloud > My Servers**.
2. On the My Servers portal page, click the name of the virtual machine to display the Take Action panel.
3. Click the **View Snapshots** icon to open the View Snapshot form

Deleting a Snapshot

1. Choose **My Cloud > My Servers**.
2. On the My Servers portal page, click the name of the virtual machine to display the Take Action panel.
3. Click the **Delete Snapshot** icon to open the Delete Snapshot form.
4. From the Snapshot name drop-down list, choose the snapshot to which you want to revert the chosen virtual machine.
5. Click **Submit Order**.

You will receive an email on the snapshot of the virtual machine that is deleted now.

Working with Virtual Data Centers

Creating a Virtual Data Center

A virtual data center (VDC) can be used by server owners in an organization to provision virtual servers. Virtual data centers live in a POD and has datastores, resource pools, and community networks as resources associated to them. Multiple virtual data centers can be ordered by an organization for server owners to provision servers in. A virtual data center has an associated size that determines limits for the number of virtual servers, vCPUs, CPU MHz, storage, and memory. Limits are enforced by comparing the sum of the number of provisioned virtual servers and the vCPUs, memory, and storage for a server size against the limits defined for the virtual data center size. A VMware resource pool is created for each virtual data center. This allows further control of resource utilization by defining CPU and memory limits, as well as CPU and memory reservations in the VMware resource pool.

You must be either an Organization Technical Administrator or Cloud Provider Technical Administrator to create a virtual data center. Create Virtual Data Center ordered by an Organization Technical Administrator requires authorization by the Cloud Provider Technical Administrator.

Note: It is not possible to add a VDC if the datacenter does not have a cluster. Cisco IAC does not support data centers with 1 host (no cluster).

The following procedure shows an Organization Technical Administrator ordering a virtual data center. If the Cloud Provider Technical Administrator orders the Create a Virtual Data Center service, all the fields that are available during authorization moment will be visible during the ordering moment and the requisition will not wait for the authorization.

1. Choose **My Cloud > My VDCs**.
2. Click **Create Virtual Data Center**.
3. On the Create Virtual Data Center form:
 - a. Enter the **Tenant Name**.
 - b. Enter the **Organization Name**.
4. Then specify the following information:
 - a. **VDC Name:** Enter a descriptive name for the virtual data center. This name will be displayed when the server owners choose the virtual data center.
 - b. **Description:** Enter a description for the virtual data center.
 - c. **Community VDC:** Choose the size of the virtual data center. The size determines the maximum limits for the number of virtual servers, maximum number

- d. **Size:** Choose the size of the virtual data center. The size determines the maximum limits for the number of virtual servers, maximum number
- e. **Compute POD:** Choose the POD in which to place the virtual data center.
 - The fields on the form will change dynamically in response to the choice you make. Complete the corresponding fields.
- f. For vCloud Director VDCs, you have two additional options:
 - **Thin Provisioning** (default is True)
 - **Fast Provisioning** (default is False)

5. Click **Submit Order**.

The requisition will go to the Cloud Provider Technical Administrator for approval.

Note: For information on obtaining approvals, see [Obtaining Approvals for Creating a Virtual Data Center, page 152](#) in [Approvals Management, page 149](#).

Completing the VDC Details

Once you click Submit in the procedure outlined in [Creating a Virtual Data Center, page 114](#), you will be presented with an additional form, Create Virtual Data Center Service.

1. View the form to verify.
2. Click the **Requisition Number** to refresh this form until you see the form repopulate to allow you to make customizations from this form, such as choosing services using check boxes and/or buttons.
3. Drill down as needed for more information by clicking on any of the VDC Services links. To return to the Create Virtual Data Service form, click the Requisition Number.
4. Return to the My VDCs form (just close the current form) to verify that your new VDC is now listed.

Note: TIP: Choose **Show > Quick Filter** to quickly search for and bring up your new VDC by name.

Now when you go to order a VM from a template, the new VDC will be available in the VDC Name field as well as in the Deploy to Network drop-down in the Network Selection section.

Adding an OpenStack Network

Virtual Data Centers can use OpenStack networks that belong to the same OpenStack project as the VDC or public networks. Please note that network can be added to only one VDC. Your first step will be to create network in OpenStack environment in project for newly-provisioned virtual data center. The network can be marked as shared, which means that this network can be assigned to a Virtual Data Center from another project.

When provisioning OpenStack OpenStack on the fly, networks are created from the Private subnet range specified in the Tenant. For Openstack Network provisioning, Advanced Network Services should be enabled using system-wide setting. Private subnet field while on-boarding a Tenant will only be shown if Advanced Network Services is enabled at the Provider level. If you only have OpenStack and you need to do network provisioning, set ANS to YES at the Provider level and to NO at the Tenant or Organization level (to avoid provisioning virtual network devices).

Note: After you have created network we will need to discover it in Cisco IAC. For instructions on how to do so, see [Discovering OpenStack Resources, page 26](#) in [Managing Resources Using Discovery, page 25](#)

Adding a Network for an Cisco APIC-Enabled OpenStack

See [Managing Cisco APIC Connections, page 135](#) for this information and for more about managing APIC connections.

Decommissioning a Virtual Data Center

You must be an Organization Technical Administrator (OTA) or a Cloud Provider Technical Administrator (CPTA) to perform this action. Note that all networks and virtual machines must be removed from the virtual data center prior to decommissioning.

1. Choose **My Cloud > My VDCs**.
2. Locate the virtual data center in the grid, then click the VDC you want to decommission.
3. In the Manage Virtual Data Center panel, click on **Decommission VDC**.

Note: In the modal window that follows, the VDC Name field will be pre-populated with the chosen virtual data center name.

4. Click the **radio button** to confirm action.
5. Click **Submit Order**.

Calculating Virtual Data Center Size Requirements

1. Choose **Setup > VDC Calculator**.
2. Complete all four steps on the VDC Calculator.
 - **Step 1. Planned VDC VM Limit:** Enter the total number of virtual machines in the Planned VDC VM Limit field.
 - **Step 2. Planned VM Distribution:** Enter names for each VM size as well as the respective virtual machine percentages for the planned VDC VM Limit, such as “Small,” “Medium,” and “Large.”
 - **Step 3. Planned VM Configuration:** Enter respective virtual machine configuration attributes for each size you entered in **Step 3**.
 - VM Quantity
 - CPU Count
 - Memory (GB)
 - Storage (GB)
 - MHz allocated per vCPU
 - Snapshots per VM
 - **Step 4. Suggested VDC Package:** Here, CIAC returns the recommended configuration, which includes:
 - Total vCPUs
 - Total Memory (GB)
 - Total Storage (GB)
 - Total MHz
3. Close the VDC Calculator when you are done.

Modifying Virtual Data Center Size

Modify VDC size allows the virtual data center size to be increased. The VDC size can only be increased not decreased. Changing the VDC size changes the corresponding memory and CPU limits and reservations in the VMware resource pool.

1. Choose **My Cloud > My VDCs**.
2. Locate the Virtual Data Center in the grid, then click the **gear icon**  to manage the chosen server.
3. In the Manage Virtual Data Center collapsible panel, click on **Modify VDC Size**. In the modal window that follows the Name field will be prepopulated with the chosen virtual data center name. The current size and size settings populate the remaining fields.
4. Choose a new size from the VDC Size drop-down list.
5. Change the Maximum Snapshots per VM, CPU Reservation (MHz), and/or Memory Reservation (GB).
6. For vCloud Director VDCs, you have two additional options:
 - a. **Thin Provisioning** (default is True)
 - b. **Fast Provisioning** (default is False)
7. Click **Submit Order**.

Viewing Virtual Data Center Details

1. Choose **My Cloud > My VDCs**.
2. Locate the Virtual Date Center in the grid, then click the name.

There is a tab panel at the bottom of the page. When you choose a virtual data center, the Virtual Data Center Details tab is displayed. There are three sections in this tab:

- **Virtual Data Center Details** shows the following details for the chosen virtual data center:
 - Name of the virtual data center
 - The POD associated to the chosen virtual data center
 - The Cluster associated to the chosen virtual data center (NOTE: Only visible to the Cloud Provider Technical Administrator)
 - The Datastore associated to the chosen virtual data center (NOTE: Only visible to the Cloud Provider Technical Administrator)
 - The Resource Pool associated to the chosen virtual data center (NOTE: Only visible to the Cloud Provider Technical Administrator)
 - The amount of CPU (MHz) Reservation associated to the Resource Pool in which the virtual data center is located (Only visible to the Cloud Provider Technical Administrator)
 - The amount of Memory (GB) Reservation associated to the Resource Pool in which the virtual data center is located (Only visible to the Cloud Provider Technical Administrator)
 - The CPU limit (MHz) associated to the chosen virtual data center
 - The total number of allocated Virtual Machines versus the total number of available Virtual Machines within the chosen virtual data center.

- The total number of allocated Virtual CPUs (MHz) versus the total number of available Virtual CPUs (MHz) within the chosen virtual data center.
- The total number of allocated Memory (GB) versus the total number of available Memory (GB) within the chosen virtual data center.
- The total number of allocated Storage (GB) versus the total number of available Storage (GB) within the chosen virtual data center.
- The maximum number of snapshots allowed within the chosen virtual data center.

If any of the above fields are blank, no data to display will be shown.

■ **Network**

- Lists the total number of networks associated to the chosen virtual data center.
- Lists the name of each individual network when there are networks associated to the chosen virtual data center.

■ **Network IP Address Utilization**

- A pie chart displaying the total number of all the IP addresses assigned and all the IP addresses that are unassigned. (

If the values of both assigned and unassigned are zero, then no pie chart will be displayed. In its place, you will see the text, “No data to display.”

Viewing Virtual Data Center Capacity Charts

To view charts depicting allocated resources versus total available for allocation:

1. Choose **My Cloud > My VDCs**.
2. Locate the Virtual Data Center in the grid, then click the arrow next to the name.
3. Click the **Usage** tab.

The following charts will populate:

- A pie chart showing network IP address utilization.
- A bar chart showing virtual machines (VMs) allocated. Hover to view additional information.
- A bar chart showing VM CPUs (MHz). Hover to view additional information.
- A bar chart showing the VM Memory (GB). Hover to view additional information.
- A bar chart showing VM Storage (GB). Hover to view additional information.



Network Provisioning

Cisco Intelligent Automation for Cloud 4.2 provides two options for using existing networks and provisioning new networks. First, you can define a network using existing port group files. Second, you can auto-provision a network using new port groups.

Note: In 4.2, Cisco Intelligent Automation for Cloud now provisions new networks on-the-fly, as it did for vCenter networks in Cisco IAC 4.0/4.1.

Defining a Network Using Existing Port Group Files

Viewing the List of All Networks

To view a list of your networks and IP capacity information for each network:

1. Choose **Operations > Network Management**.

You will see a portal displaying your networks.

2. Choose a network to view the IP Address Assignments.

Viewing the IP List for a Specific Network

Sometimes you need to view only IP capacity information for a specific network rather than for all available networks.

1. Choose the radio button next to the network for which you want to view information.
2. The list of IPs appear in the IP Address Assignments box at the lower part of the screen.

Adding a Network to a Virtual Data Center

After a virtual data center is created, Organization Technical Administrators can request additional networks for the virtual data center. Once the request is submitted, the Cloud Provider Technical Administrator must approve the request and assign a new network to the virtual data center. The network to be added must already exist. If the Cloud Provider Technical Administrator initiates the request, the CPTA can be able to directly assign a new network to the virtual data center and the request will not go for approval. To add a network to virtual data center:

1. Choose **My Cloud > My VDCs**.
2. Click the Add Network to VDC action.
3. Choose the number of hosts per network needed for the network to be added. This is used by the Cloud Provider Technical Administrator to determine which size network subnet to assign to the virtual data center.
4. Click **Submit Order**. The requisition will go to the Cloud Provider Technical Administrator for approval.

Deleting a Network from a VDC

Before you permanently remove a network, you must first remove any IP address assignments associated with the network.

1. Choose **Setup > System Settings > Networks** tab.
2. Click Remove Network.
3. On the Remove Network form, choose the network from the drop-down list.

If the network has IP addresses associated with it, an alert will inform you, and you cannot proceed with the deletion.

4. Click **Submit Order**.

Managing IP Address Exclusions

Add or remove a usage exclusion for an IP address. When an IP address is excluded, it is unavailable or off-limits for automated allocation. For example, an exclusion allows you to set aside a contiguous IP for a future use or allocate an IP address for a resource outside the Prime Service Catalog.

1. Choose **Service Item Manager** from the right-side drop-down list.
2. Click the **Manage Service Items** tab.
3. On the Manage Service Items tab, expand IP Management in the Service Items Type panel, then click **IPAddress**.
4. Locate and click the IP address in the Service Items table.
5. Click in the Usage field and change the value to one of the following values:
 - Excluded—Apply the exclusion
 - Unassigned—Remove an existing exclusion
6. Click **Save**.

Removing a Network from a Virtual Data Center

1. Choose **My Cloud > My VDCs**.
2. Locate the virtual data center in the grid, then click the **gear** icon .
3. In the popup, click **Remove Network from VDC**.
4. Choose the network you want to remove from the **Network Name** drop-down list.
5. Confirm and then click **Submit Order**.

Auto-Provisioning a Network Using New Port Groups

The Add Network Service can be used to define a network using existing port groups. If there are no existing port groups, or if users have a need for new port groups Cisco IAC 4.2 will auto-provision the port groups [port profiles for Nexus 1000v] with of the creation of the networks. Therefore, there is no need to run Add Network as a separate service. Anytime you create you delete a network, Cisco IAC 4.2 auto-deletes the newly-created port groups created as part of the auto-provision (not any of the previously-created port groups) as well.

Note: Auto-provisioning is new for Cisco IAC 4.2. Creating of new networks is supported only with Nexus 1000v.

Prerequisites

The following pools are required to be available in order to successfully auto-provision a network using new port groups:

- **Private IP Address Pool** - This is set up during the Create Tenants process (onboarding tenants) (see [Onboarding a Tenant, page 95](#)).
- **VLAN Pool** - This is set up during the Create Network Pod process. Information on creating and managing PODs can be found in the *Cisco Intelligent Automation for Cloud 4.2 User Guide*.

Managing OpenStack Volumes

You can add or delete OpenStack volumes as needed. To do so.

1. **My Cloud > My Servers.**
2. Select the **gear** icon  of an OpenStack server or instance.
3. Choose the **Modify Configuration** icon.
4. On the Modify Configuration form, update any of the fields as needed.
5. Click the hard drive (volume) icon next to the label, **Manage Volumes**.
6. The Manage Volumes popup window displays.

Attaching Volumes

1. Choose the volume to attach from the **Volumes to Attach** list.
Volume Name and **Volume Size** will be automatically populated.
2. Type the Physical Device name/path.
Note: 'Physical Device' syntax depends on the Operating System you have chosen; for Linux this is `/dev/vdd`.
3. Click **Attach**.
4. Back on the Modify Configuration form, click **Submit**.

Detaching Volumes

1. Choose the **Detach Volume** radio button.
This will activate the Volumes to detach list.
2. Choose the volume you want to detach from instance from the list.
Volume Name and **Volume Size** will be automatically populated.
3. Click **Detach**.
4. Back on the Modify Configuration form, click **Submit**.



Managing Bare Metal and Blade Pools

Checking All Prerequisites

Installing Required Software

Before you can manage bare metal blades, make sure you have the following installed and configured:

- USC Manager
- USC Director
 - USCD Bare Metal Agent

Adding Required Platform Elements to the CIAC Infrastructure

Be sure that you have added the following via Setup > System Settings > Connections tab > Connect Cloud Infrastructure:

- VMware vCenter
- USC Manager
- USC Director

Note: See [Setting Up the Infrastructure, page 41](#), for information on how to set up these (and other) platform elements.

Creating Required PODs

Ensure that you have completed the following:

- Create a Compute POD for VMware vCenter Server

Note: See [Managing PODs, page 127](#), for information on how to set up and manage PODs.

- When you create this POD, select the:
 - **Cisco UCS Manager Instance**
 - **Cisco UCS Director Bare Metal Agent**
 - **Provisioning UCS VLAN** (for physical provisioning)
 - **Provisioning Hypervisor VLAN** (for VM provisioning)

Registering a UCS Bare Metal Image

CPTAs can register a discovered UCS bare metal images in the cloud system for users to choose when ordering physical servers. The blade can be in Discovered, Maintenance, or Ignored states to be changed to Registered.

Registering a UCS Bare Metal Image

Note: Before you can register a UCS Blade, it must be discovered using the CloudSync Infrastructure Discovery portal.

1. **Setup > System Settings > Manage Cloud Infrastructure** tab.
2. Click the **Cisco UCS Director** icon.
3. Beneath this icon you will find an icon for **Bare Metal Images**. Click this icon to see the full list of bare metal images.
4. In the UCS Director BMA Images section, click the **gear** icon  next to the line item you wish to register in the grid, then click the **Register USC Director Baremetal Images** button.
5. Enter or select the following:
 - **Baremetal Image**
 - **Friendly Name**
 - **Operating System Family**
 - **Operating System**
 - **Is Hypervisor Image** (Yes or No)
 - **App Code** (user-specified by the CPTA; the string entered here will become part of the server name)
 - **Access Tenants** (All Tenants or Specific Tenants)
 - **Price**
6. Click **Submit Order**.

Registering a UCS Blade

You need to register either a UCS blade or a UCS rack server.

1. **Setup > System Settings > Manage Cloud Infrastructure** tab.
2. Click the **Cisco UCS Manager** icon.
3. Beneath this icon you will find an icon for **UCS Blades**.
4. Click this icon to proceed.
5. In the UCS Blades form, click the **gear** icon  next to the line item you wish to register in the grid, then click the **Register Cisco USC Server** button.
6. Select the **Pool Type**:
 - **Physical**
 - **Virtual**
7. Click **Submit Order**.

Registering a UCS Rack Server

You need to register either a UCS blade or a UCS rack server.

1. **Setup > System Settings > Manage Cloud Infrastructure** tab.
2. Click the **Cisco UCS Manager** icon.

Registering a UCS Bare Metal Image

3. Beneath this icon you will find an icon for **UCS Rack Server**.
4. Click this icon to proceed.
5. In the UCS Racks section, click the **gear** icon  next to the line item you wish to register in the grid, then click the **Register Cisco USC Server** button.
6. Select the **Pool Type**:
 - **Physical**
 - **Virtual**
7. Click **Submit Order**.

Understanding the Blade Registration Process

When a blade is first registered, it is placed into the Maintenance pool in the Available state. After registration, the CPTA manages blades using pool type Virtual or Physical. There are three pool types:

- **Maintenance**—A holding area for blades that are registered but have not been identified for some reason. Blades in the maintenance pool are owned and managed by Cloud Provider Technical Administrators and are not available to Server Owners.
- **Virtual**—Blades in this pool have been identified for hosting virtual machines. They have been provisioned with VMware ESXi. Blades in this pool never carry a status of Available, only In Use or Pending.
- **Physical**—Blades in this pool have been assigned for use by Server Owners. They can carry a status of Available, In Use, or Pending.

Each registered UCS blade is in one of the following statuses:

- **Available**—The blade is unassigned and not in use; it is available for physical server provisioning or VMware ESXi provisioning.
- **In Use**—The blade is assigned and in use by either a Server Owner (running Windows or Linux) or a Cloud Provider Technical Administrator as a VMware ESXi host.
- **Pending**—A physical or VMware ESXi server on the blade is provisioning.
 - For a provisioning physical server, the blade is in the physical pool and is not in transition, but its status is changing from Available to Pending, or from Pending to In Use.
 - For a provisioning ESXi server, the blade is in transition from the Maintenance pool to the Virtual pool.

Installing Service Profile Templates

You also need to assign a service profile template to each bare metal server that you register.

1. Go to **Setup > System Settings > Manage Cloud Infrastructure** tab.
2. Click the **Service Profile Templates** icon.
3. In the Service Profile Templates section, click  next to the line item you wish to register in the grid, then click the **CloudSync Edit Infrastructure** button.
4. On the CloudSync Edit Infrastructure form, complete the following:
 1. Service Profile Template Name

Ordering Physical Servers

- a. FullPath
 - b. Is Hypervisor Image (Yes or No)
 - c. Display Name
 - d. Description
 - e. Access Tenants (All Tenants or Specific Tenants)
2. Click **Submit Order**.

Ordering Physical Servers

Now that you have registered your bare metal servers as shown above, you are ready to order physical servers.

1. Go to **My Cloud > My Servers**.
2. Click the **Order PS** icon to order a physical server (PS).
3. On the **Order a Physical Server** form, complete the following:
 - VDC Name
 - Physical Servers Available
 - Physical Server Friendly Name and Description:
 - Operating System Family
 - Operating System
 - Baremetal Image Friendly Name
 - OS Template Name
 - Provisioner Template Friendly Name
 - Provisioner Template Name
 - Time Zone
 - Deploy to Network
 - Remaining Addresses
 - Lease Term
 - Order Quantity
 - Administrator Password
4. Click **Submit Order**.



Managing PODs

A POD is a Point of Delivery unit. There are two types of PODs: Network PODs and Compute PODs. There are also SRCs: Service Resource Containers. In Cisco Intelligent Automation for Cloud 4.2, you can create as many PODs as your organization requires. A POD is a module or group of network, compute, storage, and application components that work together to deliver a network service. The POD is a repeatable pattern, and its components increase the modularity, scalability, and manageability of data centers. You must be logged in as a Cloud Provider Technical Administrator to create a Network POD.

Creating One or More Network PODs

Use the Register a POD service to register an installed POD and choose the instances that manage its resources, so that you can start using it in the cloud.

1. Choose **Setup > System Settings > PODs** tab.
2. On the PODs portlet, click Register a Network POD.
3. On the Create Network POD form, define the cloud infrastructure:
 - Assign a name and description.
 - This field is not editable; only one vCenter is allowed.
 - Choose the datacenter that is to serve this POD. There is a 1-to-1 mapping between data centers and PODs.
 - If the drop-down list is empty, all available data centers have been associated with a POD.
 - *Optional.* Choose the UCS Manager that is to serve this POD. There is a 1-to-1 mapping between UCS Managers and PODs.
 - If the drop-down list is empty, all available UCS Managers have been associated with a POD.
 - *Optional.* Choose the Server Provisioner instance that is to serve this POD. A CSP can be associated with multiple PODs. This option requires:
 - vCenter Port Group for OS Provisioning - The port group inside the vCenter that will be used for the provisioning VLAN for bare metal installations.
 - UCS VLAN for OS Provisioning - The VLAN associated with UCS that is used by the Server Provisioner for bare metal installations.
4. Click **Submit Order**.

Modifying Network POD Properties

1. Choose **Setup > System Settings > PODs** tab.
2. On the PODs portlet, click Modify a Network POD.
3. On the Modify Network POD form, complete the fields, as needed.

Removing a Network POD

- Network POD Name and Description
 - VLANPool
 - Edge Router
 - Layer3 Aggregation Switch
 - Layer3 Service Node
 - Layer2 Access Switch:
 - UCS Manager Interconnect
 - Virtual Access Switch
4. Click **Submit Order**.

Removing a Network POD

1. Choose **Setup > System Settings > PODs** tab.
2. On the PODs portlet, click Remove a Network POD.
3. On the Remove Network POD form, choose the POD from the drop-down list.
4. Check the **YES** check box next to **Confirm Action**.
5. Click **Submit Order**.

Working with Compute PODs

1. Choose **Setup > System Settings > PODs** tab.
2. Click **Register a Compute POD**.
3. On the Create Compute POD form, do this:
 - Enter a new short name for the Compute POD.
 - *Optional.* Enter a **Description** for the POD.
 - Choose the Cloud Infrastructure Type from the drop-down list. Options include:
 - Amazon EC2
 - Cisco Unified Computing System (UCS) Director
 - OpenStack Cloud Manager
 - VMware vCenter Server
 - VMware vCloud Director
4. Depending on the type you choose, you will see additional options. For example:
 - For OpenStack Cloud Manager, you would see:
 - Network Pod Name
 - OpenStack Cloud Manager Instance

- For VMWare vCenter server you see:
 - Network POD, VMware vCenter Instance
 - VMware Datacenter
 - Cisco UCS Manager Instance
 - Provisioning UCS VLAN
 - Provisioning Hypervisor VLAN
- In other cases, you may just see one or two additional fields.

5. Click **Submit Order**.

Note: At this point, you are now able to create a virtual data center (VDC).

Modifying a Compute POD's Properties

1. Choose **Setup > System Settings > PODs** tab.
2. Click **Modify a Compute POD's Properties**.
3. On the Remove Compute POD form, choose the POD from the drop-down list.
4. Check the YES check box next to **Confirm Action**.
5. Click **Submit Order**.

Removing a Compute POD

1. Choose **Setup > System Settings > PODs** tab.
2. Click **Remove a Compute POD**.
3. On the Remove Compute POD form, choose the POD from the drop-down list.
4. Check the YES check box next to **Confirm Action**.
5. Click **Submit Order**.

Working with Service Resource Containers

Creating a Service Resource Container

1. Choose **Setup > System Settings > PODs** tab.
 2. Click Create a Service Resource Container.
 3. On the Create Service Resource Container form, complete the required fields.
- **Create Service Resource Container**
 - Give a friendly name to easily identify the set of resources allocated for network services.
 - Choose a Compute POD, Datacenter Name, Cluster Name, and Datastore Name

- Infrastructure Network: Choose a network to which management interface of the Network Service Virtual Machines will be connected.
 - Service Network: Choose a network to which service interface of the network service virtual machines will be connected.
 - Internet Transit Network: Choose a network to which Internet interface of the Virtual Network Service nodes will be connected.
- Application Configuration Management
- Choose the Chef or Puppet radio button and then complete one of the following, as applies:
- Chef Target Name: Choose from available Chef connections
 - Puppet Target Name: Choose from available Puppet connections

You can only choose either one Chef or one Puppet PE Target per Service Resource Container in the SRC form. In other words, one or the other but not both.

- Resources (Resource Pool:
- Enter the Resource Pool Name and Description
 - CPU Shares: Choose CPU shares for the Network Service Virtual Machines.
 - CPU Limit (MHz): Enter the CPU Limit in MHz for the resource pool. Enter -1 for unlimited.
 - Memory Limit (GB): Enter the MemoryLimit for the resource pool. Enter -1 for unlimited.
 - CPU Reservation (MHz): Enter the amount of CPU reservation in MHz to exclusively set aside for this resource pool.
 - Memory Reservation (GB): Amount of memory to exclusively set aside for this resource pool.

The above fields will be somewhat different based on Compute POD chosen. The heading for this section changes as well, such as “Resource Pool” or “OpenStack Resources.”

4. Click **Submit Order**.

Modifying Service Resource Container Properties

Modify assigned resources for a registered Service Resource Container.

Note: Modifying Service Resource container will be slightly different from the steps outlined below if you are modifying resource container for OpenStack POD. There will be additional OpenStack-specific fields.

1. Choose **Setup > System Settings > PODs** tab.
 2. Click **Modify Service Resource Container Properties**.
- Choose a Resource Name and enter the ClusterName
- Modify as needed:
- POD Name
 - Datacenter Name
 - Cluster Name
 - Datastore Name

- Management Network
 - Service Network
 - CSR Organization
 - VSG Organization
 - VPX Organization
- For the Resource Pool, modify any or all:
- Resource Pool Name and Description
 - CPU Limit (MHz): Enter the CPU Limit in MHz for the resource pool. Enter -1 for unlimited.
 - Memory Limit (GB): Enter the MemoryLimit for the resource pool. Enter -1 for unlimited.
 - CPU Reservation (MHz): Enter the amount of CPU reservation in MHz to exclusively set aside for this resource pool.
 - Memory Reservation (GB): Enter the amount of memory to exclusively set aside for this resource pool.

If Service Resource Container was created without an applications server assigned to it, it is possible to assign a container using the Modify Service Resource Container Service.

3. Click **Submit Order**.

Deleting a Service Resource Container

Remove a Service Resource Container and disconnect all infrastructure resources associated to the container.

1. Choose **Setup > System Settings > PODs** tab.
2. Click **Delete a Service Resource Container**.
3. On the Delete a Service Resource Container form, choose the POD from the drop-down list.
4. Check the **YES** check box next to **Confirm Action**.

Note: For OpenStack, removing a service container will remove the project from your OpenStack environment.

5. Click **Submit Order**.



Managing vApp Containers

You can create, manage, modify, and delete VMware vCD vApps within Cisco Intelligent Automation for Cloud 4.2.

Creating a Containers

A vCloud vApp is created from a template, and includes the enclosed VMs.

Note: A vApp is a vCloud Director container.

1. Go to **My Cloud > My Containers**.

- You will see a list of current containers, if any.

2. Click **Create Container**, the button at the top left of the screen. This opens the **Create Container from Template** form.

Tip: You can also access this form via **My Cloud > My VDCs**. Select the **gear** icon  next to the VDC you want to use. From the  popup, select **Create vApp from Template**.

3. Select the **VDC Name** for the Virtual Data Center upon which to deploy the vApp.

Note: If selected from My VDCs, the VDC Name is not selectable. Instead, it reflects the VDC from where you originally entered the form.

4. Enter the **vApp Name**.

5. Enter an optional **vApp Description**.

6. Select the **vApp Template**.

Note: vCloud Director has a number of vApp and VM templates for you to choose from.

7. Select the **Network**.

8. Click **Submit Order**.

Managing Containers

- Use the triangle (▶) next to the container name to view any VMs associated with the container, with information such as the name, the OS installed, and so on.
- Use the **gear** icon  next to the container to:
 - Power Up Container
 - Power Down Container
 - Restart Container
 - Decommission Container

Note: Selections of the individual icons will be available only when applicable.

Decommissioning a Container

When you decommission a container, the following happens:

- All of the VMs within the container are turned off
- All of the VMs are then deleted
- Finally, the vApp itself is deleted

Viewing VMs Within Containers from My Servers

1. Go to **My Cloud > My Servers**.
2. Scroll to find the VM you are interested in.

Note: Any VM with a VMware vCloud Director icon in the VM column is a VM within a vApp container.

- You can do anything with container VMs that you can with other VMs using the **gear** icon .
- In addition, you can clone the VMs within a vApp to another vApp.

vApp Container Pricing

A vApp is basically a container. A vApp template will contain one or more VMs. Pricing is done per VM. So, for example you might have an **XS** (extra small) VM set at \$20, an **S** (small) VM set at \$25, and so on. (You may have noticed just now that Cisco IAC uses “tee shirt sizes” for VMs.)

So, for any given vApp template in use, Cisco IAC has no way of knowing the sizes and amounts for the VMs contained within it. Therefore, for pricing within vApps, charges are for the full container, rather than for individual VMs.

1. Go to **Setup > Manage Infrastructure**.
2. Scroll the list on the left-hand side and choose **VMware vCloud Director**.
3. Choose **vApp Templates**.
4. On the vCloud vApp Templates page, select the **Gear** icon next to the vApp template you want to register.
5. From the popup, choose **Register vCloud vApp Template**.
6. On the Register vCloud vApp Template form, complete the following:
 - a. Enter an optional **Description**.
 - b. Give the template a **Friendly Name**.
 - c. Choose access type (**All Tenants** or **Specific Tenants**).
 - d. In the **Price** field, enter the price for this vApp container.

Note: The VMs within this template will not be priced separately, but will be included in the price of the container.

7. Click **Submit Order**.

Note: You will see on the Modify VMs page (My Cloud > My Servers > Order VM) that the option to modify the size/price of the VMs within a container is not available ( > **Modify Configuration**), because prices are now at the vApp level and not for the separate VMs. In addition, you cannot clone a vApp, like you can a VM ( > **Clone VM to vApp**).



Managing Cisco APIC Connections

Important: For more information, refer to detailed Cisco APIC documentation located here:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/api/openstack/b_Cisco_APIC_OpenStack_Driver_Install_Guide.html.

Connecting APIC as a Platform Element (PE)

Your first step is to connect the Cisco APIC platform element using the Connect Cloud Infrastructure. To do this, you follow the same provisioning procedure as all the other platform elements. See [Defining the Cisco Application Policy Infrastructure Controller \(Cisco APIC\) Platform Element, page 44](#) for more information

Note: Updating the APIC PE would be also following the update procedure for IAC PEs.

Creating a VDC for the OpenStack APIC-Enabled Cloud Platform

To create a VDC for the OpenStack APIC-enabled cloud platform, follow the same setup steps as you would for creating any VDC. See [Working with Virtual Data Centers, page 114](#) for more information.

Note: We recommend that you use “APIC” somewhere in the name of the VDC you are creating for APIC.

Creating a Network in OpenStack VDC APIC-Enabled.

Create the OpenStack VDC APIC-enabled network and subnet as you would normally. This one will be APIC-enabled. See [Provisioning and Managing Networks, page 105](#) for more information.

Note: For more information, refer to detailed APIC documentation located here:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/api/openstack/b_Cisco_APIC_OpenStack_Driver_Install_Guide.html.

Creating the Cisco APIC Network Policy

To create an APIC Network Policy you perform the following steps.

1. Select **My Cloud > My VDCs**.
2. On the My VDCs page, find the OpenStack APIC-enabled VDC you want to provision an APIC network policy for.
3. Select the **gear** icon  next to the OpenStack VDC.
4. From the popup, select the **APIC - Create Network Policy** icon.
5. Fill in the selectable fields on the Create Network Policy form, under the APIC Network Policy Details section.

Note: Some fields have pre-populated default values that cannot be changed in Cisco IAC 4.2.

- a. **APIC Application Profile Name:** This is the name of the APIC Application Profile associated with the VDC.
- b. **Action:** The action to be taken on the filtered traffic, such as “Allow”.

- c. **VDC Name:** The VDC name.
- d. **Source Network Name:** Name of the network that is associated with the APIC Endpoint Group that *provides* the contract's traffic filtering rules.
- e. **Destination Network Name:** Name of the network associated with the APIC Endpoint Group that *consumes* the contract's traffic filtering rules.
- f. **Contract Name:** "Default" is the only contract available with Cisco IAC 4.2.

6. Click **Submit Order**.

Note: This request is a direct call to APIC Northbound API. APIC will then translate to low level network policies and apply them to the ACI fabric for traffic filtering.



Managing Applications

Cisco Intelligent Automation for Cloud 4.1 now includes applications management. With Application Provisioning support, you can now manage your applications per server or virtual machine (VM):

- When ordering a VM (BootStrapping)
- After ordering a VM (Brownfielding)

Cisco Intelligent Automation for Cloud now allows for Bootstrap Provisioning—application provisioning for virtual servers.

Note: Either a Puppet or Chef agent is automatically bootstrapped onto the VM being provisioned. These agents are pulled from the Cisco IAC Management Appliance's image repository.

Note: You can enable Application Configuration Management (ACM) at the organization, tenant, or system-wide levels.

Managing Applications

1. Choose **My Cloud > My Servers**.
2. From the server list, click the **gear** icon  next to the server you want to manage applications for.
3. Click **Manage Application**.
4. Complete the Manage Applications form:
 - Choose the environment.
 - Enter the administrative login.
 - Enter the administrative password; re-enter to confirm.
 - Move chosen applications to and from the server using
 - Available Applications
 - Chosen Applications
5. Click **Order**.

Viewing Application Servers

In Cisco Intelligent Automation for Cloud 4.1 you can monitor application usage using the My Applications dashboard.

1. Choose **My Cloud > My Applications**.

The My Applications form shows you:

- Applications available in the environments
- Number of VMs running the application
- Application price

Viewing the Applications Dashboard

- Revenue received from this application to-date
- 2. Choose the triangle next to the application you want to view.

A table displays showing you:

- Associated Servers
 - Environments
 - Infrastructure
3. Drill down on All Servers to view the servers associated with the application.
 4. Drill down on All Environments to view the environments associated with the application.

Viewing the Applications Dashboard

1. Choose **My Cloud > My Applications**.
2. Choose the Dashboard button to the right of the screen.

Here you can see Dashlets aggregating total use of application across cloud platforms. Categories are Applications By Configuration Type and Application Use.

Note: The aggregated views are available only to CPTAs.

3. You can toggle between Chart and Data views for both data types.
4. Close the dashboard when you are done.

About the Dashlets

Note: There are only two dashlets: Applications By Configuration Type and Applications Use. The Applications Use dashlet also appears on the Tenant Management dashboard.

Dashlets are available by configuration type: Chef or Puppet. The dashlets display:

- The total available servers,
- Servers/nodes in use, and
- The applications on each of the servers

Note: For information on application pricing, refer to [Financial Management, page 99](#).



Managing Alerts

You can add, modify, and delete service alerts on OpenStack virtual machines (VMs) in Cisco Intelligent Automation for Cloud 4.2. Notifications are sent via email only in Cisco IAC 4.2.

Viewing Alerts

Alerts display on the Cisco IAC 4.2 tool bar, to the left of your ID. In the alerts icon shows the total number of active alerts. The icon is color-coded as well to indicate severity level. Red is Critical, yellow means Minor, and orange indicates Major or a mix of severity levels.

To view the alerts, click on the icon. You can use the tabs at the top of the popup to view All of the alerts, or just Critical, Minor, or Major alerts separately.

Defining (Creating) an Alert

You define a new alert, also known as an alarm, via My Servers.

1. Choose **My Cloud > My Servers**.
2. Click on the **gear** icon  next to the server that you want to create an alarm for.
3. Click the **Alarms** icon.

The current alarms display on the Alarms page.

4. Click the **Alarm Definition** tab.
5. Click the **+** to define a new alert/alarm.
6. In the Create Alert Threshold popup, give the alert a name and a description and click Next.
7. Choose Alert Severity from the drop-down list. Options include:
 - Critical
 - Major
 - Minor
8. In the Trigger When drop-down, choose a metric. Metrics include:
 - CPU Utilization
 - Memory Usage
 - Disk Read
 - Disk Write

Note that this drop-down is followed by the words “is greater or equal to.”

9. In the blank field, enter the correct amount based on your selection in Trigger When.

Modifying an Alert

- Options are either % (for CPU) or **GB** for the other options.
- 10. Enter a related number in the Clear When field.
Note: The clear value should be less than the trigger value.
- 11. Enter the number of occurrences in the Duration field.
- 12. Choose a Period. Options include:
 - 1 Minute
 - 15 Minutes
 - 5 Minutes
 - Daily
 - Hourly
 - Monthly
 - Weekly
- 13. Click **Next**.
- 14. Enter a valid email address(es) in the Notification field.
- 15. Click **Save**.

Modifying an Alert

1. Choose **My Cloud > My Servers**.
2. Click on the **gear** icon  next to the server that you want to create an alarm for.
3. Click the **Alarms** icon.
Note: The current alarms display on the Alarms page.
4. Click the **Alarm Definition** tab.
5. Click the **+** to define a new alert/alarm.
6. In the Create Alert Threshold popup, give the alert a name and a description.
7. Click **Next**.
8. Modify the alert definitions as needed.
9. Click **Next**.
10. Click **Save**.

Deleting an Alert

1. Choose **My Cloud > My Servers**.
2. Click on  next to the server that you want to create an alarm for.
3. Click the **Alarms** icon.

Deleting an Alert

Note: The current alarms display on the Alarms page.

4. Click the **Alarm Definition** tab.
5. Highlight the alert you want to delete.
6. Click the **X** to delete the alert/alarm.



Error Remediation

For error remediation in Cisco IAC 4.2, use the Error Remediation Queue.

Viewing Errors

1. Go to **Operations > Error Remediation**.

The Error Remediation form displays.

2. To find the error in question, from the Error Remediation portlet enter information into one of the following:

- Requisition ID
- A Service Name
- Severity
- Count
- Alert Date
- Order Date
- Ordered By
- Tenant Organization
- Last Action Taken

3. Press ENTER

Depending on the data type you chosen, the data will filter, reorder. Find the record you searched for in the results. ERS data can be filtered by Remediation Status field values (such as Ongoing, Cancel, and so on). The filter is located at the top right corner of the page.

Note: If you use Requisition ID, the results will be a single record for that ID if it exists.

Viewing and Analyzing Errors

1. Choose **Operations > Error Remediation**.
2. The Error Remediation Portlet displays.
3. For the error you are interested in, click the triangle icon.
4. Read through the information displayed to analyze the error.
5. Click on any of the **links** to drill down for additional information.
6. Take necessary action on these additional info screens, as needed.
7. Close the screens when done.

8. Proceed to Remediating Errors to take action.

Remediating Errors

If you ever receive an e-mail notification of a discovery error related to a platform element you defined, follow the instructions in this section to remediate the error.

1. Choose **Operations > Error Remediation**.
2. The Error Remediation Portlet displays.
3. To remediate an error, click the **gear** icon  next to the error you want to fix.
4. From the Remediation pop-up, click one of the following, as appropriate.
 - **Cancel**—(Always available) Halt the service immediately and take no further action. No cleanup or verification of the integrity of data is performed.
 - **Restart**—Performs a Cancel followed by Restart. To do a rollback it requires a special rollback flag set in the ERS instrumentation. The flag is set to *False* by default.
 - **Retry**—Attempts to resume service fulfillment at the step that failed. A retry of the step is executed from a start point set in the service orchestration.
 - **Ignore**—Attempts to resume service fulfillment, skipping the step that failed.
 - **Rollback**—Relinquishes all resources, all infrastructure and service item changes are reversed, and restores the cloud to the state prior to the service fulfillment request. In the case of Restart, the Rollback flag is set to true, so a Rollback is getting executed on Restart.
5. Choose to send an email (optional).

Note: Sending an email is only available for Cancel and Rollback operations. It will send an email to the end user who submitted the request that the request did fail.
6. Close the popup.

Handling Infrastructure Errors

As a Cloud Provider Technical Administrator, you are entrusted with maintaining the cloud system and ensuring maximal uptime. If problems arise with fulfillment of a customer's requisition (for example, a new virtual machine), you receive an email notification error with error code, Description, automation summary link and link to the Cloud Service Errors portlet. Service problems can arise in any of the following conditions:

- Blade error has disabled all VMs running on it
- Blade error has occurred on a physical blade
- Cisco UCS Manager, VMware vCenter, LDAP server, or blades in the physical pool have failed
- Connection is lost
- Capacity has reached the maximum limit

The notification will identify the failing service and provide any or all of the following information:

- Automation summary
- Steps you must take to fix the problem, such as:

Remediating Errors

- Performing a roll-back and clean-up of the service to free up and reset associated resources, cancel the requisition, and re-order the service from Prime Service Catalog
 - Taking manual actions outside the system
 - Restarting the process from Prime Service Catalog
 - Canceling certain actions in-flight if necessary
- Referral to a knowledge base article that provides tips and best practices that you can use to determine the actions to take to recover the process

After the correction, Process Orchestrator automatically makes a second attempt to run the service. If the second attempt fails, you must cancel the order, then notify the requester to resubmit the order.

Assigning the Remediation Task for Repair

When a service requires remediation, it is automatically added to the Cloud Service Remediation queue in Service Manager. You receive the notification of failure, then assign yourself or another Cloud Provider Technical Administrator to address the issue. View the Cloud Service Remediation queue and assign a task using the following steps:

1. Choose **Service Manager** from the module drop-down list.
2. In the left navigation panel on the Service Manager Home page, expand All Queues in the tree on the left-hand side, then click the *name* (not the radio button next to) **Cloud Service Remediation**. Unassigned tasks appear in a list.
3. In the Cloud Service Remediation queue list, click the requisition number. Display-only summaries of the task and requisition appear below the Cloud Service Remediation queue.
4. Assign the task:
 - To assign the task to yourself, choose **Check Out** from the More Actions drop-down list. The task is moved to the My Work view in the left navigation panel.
 - To assign the task to someone else, expand Service Teams in the tree on the left-hand side, then the team to which the user belongs, click the radio button by the user's name, then click **Assign**. The task is moved to the chosen person's My Work view; the person is notified of the assignment.

Note: After the task is assigned, the assignee must first check out the task from the Cloud Service Remediation queue before fixing the failure.

Remediating a Service

After you have checked out the task (see [Assigning the Remediation Task for Repair, page 145](#)) from the Cloud Service Remediation queue, remediate the issue and initiate continuation of the fulfillment process.

Note: To free up the reserved resources, attempt to remediate the issue, even if you know or suspect the attempt will fail. You should not cancel the order unless your attempt to remediate the issue is unsuccessful.

1. Choose **Operations > Error Remediation**.

The table displays information such as requisition ID, the name of the service with errors, severity of the error, date when the service was ordered, and last action taken on the service.

2. Choose the service that is assigned to you and needs action.
3. Choose one of the following options from the **Remediate Error** panel to remediate the service. (Click the **gear** icon  to access.)

Remediating Errors

- **Cancel** - Stops the service delivery in its current state. Any changes in the portal will not be changed or cleared when you cancel a service. For example, service “Take Snapshot” fails. You can choose to cancel the service. If your attempt to remediate the issue fails to complete the service, you must terminate the service to release the resources that may be tied up by the stalled process
- **Restart** - Available for every service. This action will undo any changes to the service and attempts to start over from the beginning of the order.
- **Retry** - Available for every service. This option attempts to resume service at the step that just failed. For example a service “Commission VM from Template” fails because vCenter server was down. You could then retry to reach the server again.
- **Ignore** - Attempts to ignore the step that just failed and continues with the next step in the process. For example a service “Server Provisioning” fails at customize VM activity and the server is partially provisioned at this step. You could choose to correct the error manually and ignore this step.
- **Rollback** - Available for every appropriate service. This option reverses all infrastructure and service item changes. For example, a service “Commission VM Template” service fails because the datastore is full or you want to change the form data. You could rollback to reverse any or all the changes that you made to the service and then cancel the order. Thus, the service could be at its starting point after a Rollback while you continue to create a new order.

4. Perform the necessary steps to remediate the issue.

5. After remediating the issue, click **Submit Order**. This action changes the status of the task to *In Progress*, and initiates continuation of the fulfillment process.

If the delivery process is successful, proceed to the next section, [Checking the Status of an Order, page 146](#). If the delivery process is *not* successful, the requisition will appear in the Cloud Service Cancellation queue. Skip to [Canceling the Order if Remediation Attempt is Unsuccessful, page 146](#).

Checking the Status of an Order

If the delivery process is successful, then the ordered service will be fulfilled and the requisition status changed to Complete, and no further action is needed. To check the status:

1. Return to the Service Manager Home page and click **Cloud Service Delivery Management** under All Queues in the left-hand panel.
2. Locate the requisition in the queue, then click the requisition number to open the Task Data page.

Note: The status is listed in the Service Information panel.

Canceling the Order if Remediation Attempt is Unsuccessful

To free up the reserved resources, attempt to remediate the issue before canceling the order, as instructed in [Remediating a Service, page 145](#), even if you know or suspect the attempt will fail. Cancel the order *only* if your remediation attempt is unsuccessful. If your attempt to remediate the issue fails to complete the service, you must terminate the service to release the resources that may be tied up by the stalled process.

1. On the Service Manager Home page, click **Cloud Service Cancellation** under All Queues in the left-hand panel.
2. Locate the requisition in the queue, then click the requisition number to open the Task Data page.
3. Click **Cancel**. This action terminates the order and change service status to cancelled.



Approvals Management

Authorizations are any approvals required in conjunction with completing fulfillment of a service request. Authorizations give the approver the opportunity to determine if the person requesting the service is eligible to receive it.

If an authorization is rejected, the requisition will be canceled and the service will not be delivered. A requisition that needs authorization will be placed in a queue specifically created for approvals. A queue for approvals is created whenever a new organization is created.

Both the Organization Technical Administrator and the Cloud Provider Technical Administrator will have permissions to perform approve or reject actions on a service requisition that needs approval. Every requisition that needs approval waits in the queue until it is either approved or rejected. Performer of the approvals will be notified whenever a requisition that needs approval enters the approval queue.

When a requisition is rejected, email notification will be sent out to the requester of the service. No notification will be sent out when a requisition is approved.

- Approvals needed by the Cloud Provider Technical Administrator will go into the queue created by default for the Cloud Provider Organization.
- Approvals needed by Organization Technical Administrator will go into organization-specific queues. These are the naming convention for the queues:

Organization	Queue
Cloud Provider Organization	Cloud Service Approval Administration
Other	Approvals for <Organization Name>

Approvals are mandatory for the following services and are automatically enabled:

Service	Cloud Provider Administrator Approval is Required	Organization Administrator Approval is Required
Create Virtual Data Center	Yes	No
Add Network to VDC	Yes	No

Managing Approval Requests

Using the Approvals Portlet

Use the Approvals portlet to track and view authorizations for service requisitions—and thereby control expensive or resource-intensive services. The Approvals portlet displays a list of authorizations filtered by authorization type and authorization status.

Both the Organization Technical Administrator and the Cloud Provider Technical Administrator can use the Approvals portlet to approve, cancel, or reject a service requisition; a service requisition that needs approval waits in the queue until it is either approved or rejected. The service requester will be notified through email when the service waits for approval and gets the notification when a service is rejected.

For information about using the Approvals portlet to track and view authorizations, see the “Approvals Portlet” section in the [Cisco Service Portal 9.4 Designer Guide](#). You can also access the Approvals portlet from the module drop-down list; choose **Service Portal**, then click the **Approvals** tab.

Note: The Service Manager module can also be used to manage approvals. For more information about the Service Manager, see the [Cisco Service Portal 9.4 Configuration Guide](#).

Approval Queues

Services that need approvals will be placed in the corresponding queues:

- Approval needed by the Cloud Provider Technical Administrator will be placed in the Cloud Service Approval Administration queue.
- Approval needed by Organization Technical Administrator will be placed in the queue with the naming convention Approvals for <Organization name>.

Accessing the Approvals Queue

For approval management, use the Approvals Queue.

1. Choose **Service Portal > Operations > Approvals**.
2. The Approvals Portlet displays.

Viewing and Analyzing Approvals

1. View the approvals. The icons next to each approval request indicate its status.
2. Use the **+** sign to open a panel showing additional status information such as:
 - Approved
 - Canceled
3. Click on any **Order number** in the list to view task details, such as:
 - Requisition Number
 - Customer
 - Customer E-Mail
 - Customer Work Phone
 - Organizational Unit
 - Status
 - Initiator
 - Created Date
 - Submit Date
 - Closed Date
 - Status
 - Follow Up

- Started On
 - Completed On
 - ... and so on.
4. Close the screen when done.
 5. Close the Approvals portlet.

Configuring Approvals

1. Choose **Setup > System Settings > Approvals** tab.
2. Click **Configure Approvals**.
3. On the Configure Approvals portlet page, choose a Service.
4. Choose **Yes** or **No** for each of the following:
 - a. Cloud Provider Technical Administrator Approval
 - b. Cloud Provider Business Administrator Approval
 - c. Tenant Technical Administrator Approval
 - d. Tenant Business Administrator Approval
 - e. Organization Technical Administrator Approval
5. Click **Submit**.

Obtaining Approvals for Create Virtual Data Center

When an Organization Technical Administrator submits a requisition for Order a Virtual Data Center, it goes to the CPTA's Cloud Service Approval Administrator queue for approval. The Cloud Provider Technical Administrator must assign a POD, cluster, datastore, and networks for the virtual data center, as part of the approval process.

1. Choose **Service Portal** from the module drop-down list; then choose **Cloud Operations > Approvals**.
2. Click the order number in the **Order #** column to create a virtual data center requisition that requires approval. This brings up the requisition form.
3. Choose the POD that this virtual data center should be created on. The POD chosen should be based on the virtual data center size chosen and available capacity in the POD.
4. Choose the cluster that this virtual data center should be created on. The cluster chosen should be based on the virtual data center size chosen and available capacity in the cluster. A single cluster can host multiple virtual data centers.
5. Choose the datastore that this virtual data center will use. The datastore chosen should be based on the virtual data center size chosen and available capacity of the datastore. A single datastore can be associated with multiple virtual data centers.
6. You can also change the CPU reservation in MHz for the virtual data center resource pool. The default value is based on the VDC Size chosen. This corresponds directly to the VMware resource pool CPU reservation.
7. You can also change the memory reservation in GB for the virtual data center resource pool. The default value is based on the VDC Size chosen. This corresponds directly to the VMware resource pool memory reservation.

Obtaining Approvals for Adding Network to VDC

8. Choose the network name that should be assigned to the virtual data center. The networks that are shown in the list are non-community, user networks. The network chosen should be based on the Hosts per Network specified in the requisition.
9. Optionally, a management network can be associated with a virtual data center. If desired, choose a management network for the virtual data center. The management network subnet size should be the same as the user network size.
10. If the virtual data center has more than one network, repeat steps 8-9 for each network.
11. Click **Update** to update the requisition with the VDC resource assignment information.
12. Click **Approve**.

Obtaining Approvals for Adding Network to VDC

After an Add Network to VDC requisition is submitted by an Organization Technical Administrator, it goes to the CPTA's Cloud Service Approval Administrator queue for approval. The Cloud Provider Technical Administrator must assign a network to the virtual data center and then approve the requisition.

1. Choose **Operations > Approvals**.
2. Click on the **Order #** for the Add Network to VDC requisition that requires approval. This brings up the requisition.
3. In the Network Name field, choose the network to be added.
4. In the Management Network field, optionally choose a management network to be associated with the community network. The management network should be the same subnet size as the community network.
5. Click **Update** to update the requisition with the VDC resource assignment information.
6. Click **Approve** for the request.

Obtaining Approvals for Creating a Virtual Data Center

When an Organization Technical Administrator submits a requisition for Order a Virtual Data Center, it goes to the CPTA's Cloud Service Approval Administrator queue for approval. The Cloud Provider Technical Administrator must assign a POD, cluster, datastore, and networks for the virtual data center, as part of the approval process.

1. Choose **Operations > Approvals**.
2. Click the order number in the **Order #** column to create a virtual data center requisition that requires approval. This brings up the requisition form.
3. Choose the POD that this virtual data center should be created on.
Note: The POD chosen should be based on the virtual data center size chosen and available capacity in the POD.
4. Choose the cluster that this virtual data center should be created on.
Note: The cluster chosen should be based on the virtual data center size chosen and available capacity in the cluster. A single cluster can host multiple virtual data centers.
5. Choose the datastore that this virtual data center will use. The datastore chosen should be based on the virtual data center size chosen and available capacity of the datastore. A single datastore can be associated with multiple virtual data centers.
6. You can also change the CPU reservation in MHz for the virtual data center resource pool.

Obtaining Approvals for Creating a Virtual Data Center

Note: The default value is based on the VDC Size chosen. This corresponds directly to the VMware resource pool CPU reservation.

7. You can also change the memory reservation in GB for the virtual data center resource pool. The default value is based on the VDC Size chosen. This corresponds directly to the VMware resource pool memory reservation.
8. Choose the network name that should be assigned to the virtual data center. The networks that are shown in the list are non-community, user networks. The network chosen should be based on the Hosts per Network specified in the requisition.
9. Optionally, a management network can be associated with a virtual data center. If desired, choose a management network for the virtual data center.

Note: The management network subnet size should be the same as the user network size.

10. If the virtual data center has more than one network, repeat steps 8-9 for each network.
11. Click **Update** to update the requisition with the VDC resource assignment information.
12. Click **Approve**.



Managing Standards

Service option standards are the options that appear in drop-down lists for users to choose when ordering servers. Using the Standards service, you can control the available lease term options by adding or modifying of these service option standards. You can add, modify, or delete the lease term, operating system, server, VDC or Shared Zone size standards for ordering servers. The values you set will appear as choices for users when ordering servers.

Viewing Standards Settings

View the default standard settings for lease term, operating systems, and server size (among other settings) to determine whether you want to change the values.

1. Choose **Setup > System Settings > Standards** tab.
2. Click **Define Order Standards**.
3. In the Standard panel on the left, move through the standards type to view settings.

Adding, Modifying, or Deleting a Lease Term Standard

Lease term standards define the lease duration options that users can choose from drop-down lists when they order servers. A lease is a service option that sets a duration (for example, three months) on a server from the time it is commissioned. During the lease period, the server is active and accessible to users. When the lease term expires, the server is automatically decommissioned and placed into storage for a defined length of time. (When a server is decommissioned, it has not been deleted, but it is not accessible to users.) When the storage period expires, the server is deleted and its data is lost. A Server Owner can extend the lease on the server while it is active, or re-commission the server while it is in storage.

Note: Lease term settings are defined in seconds. If you add or modify a lease term standard, you will need to know the number of seconds in the new lease duration. The table that follows lists seconds in hour and day units to help you calculate the values.

Each lease term standard has four settings:

- **Term**—The name of the option describing the duration of the lease. For example, 90 days. This value appears in the drop-down list for users to choose, so it must be clear and descriptive.
- **Runtime Seconds**—The duration of the lease, defined in seconds. The runtime value must always match the defined term. For example, a 30 day lease has a runtime value is 2592000 seconds. This value is hidden from users.

Note: The table that follows lists seconds in hour and day units to help you determine values for lease terms.

- **Storage Seconds**—The time period during which the server is stored after the lease expires. The default setting is 864000 seconds, or 10 days. This value is hidden from users.
- **Warning1Seconds**—The number of seconds before the lease expiration date when the first expiration warning notification is sent to the server owner. The default setting is 604800 seconds, or 7 days after commission. This value is hidden from users.

- **Warning2Seconds**—The number of seconds before the lease expiration date when the second expiration warning notification is sent to the server owner. The default setting is 86400 seconds, or 1 day before expiration. This value is hidden from users.

Adding a New Lease Term Standard

Cisco IAC ships with five pre-configured lease term standards: 30 days, 90 days, 6 months (180 days), 1 year, and No Lease. You can accept, modify, or delete a default lease term standard, and you can add a new standard.

1. Choose **Setup > System Settings > Standards** tab.
2. Click **Define Order Standards**.
3. In the Standard panel on the left, move through the standards type to view settings.
4. Click **Lease Terms** in the Service Options folder on the left.
5. Click **Add New**. An empty row appears.
6. In the Standard Data table, click inside the Term field in the new row and enter a label for a unit of time (for example, 60 days). This entry will appear to users in the drop-down list on the order forms.

Note: It is recommended that you avoid using months, because the numbers of days in months vary. Because lease durations are defined in seconds, and the seconds values would not be consistent from month to month. It is recommended that you use four-week units instead of months.

7. Click inside the **Runtime Seconds** field and enter the number of seconds in the Term duration you defined above. Do not include commas in the value.

The Runtime Seconds value must match the Term you have entered. For example, the runtime value for a 60-day lease term is 5184000 seconds. Use the figures in the following table to calculate the Term duration in seconds.

Duration	Runtime Value (Seconds)
12 hours	43200
1 day	86400
7 days	604800
28 days	2419200
180 days (about 6 months)	15552000
365 days (1 year)	31536000

8. In the Storage Seconds field, enter the amount of time, in seconds, during which the decommissioned server is held in storage. When this defined storage duration expires, the server will be deleted. The suggested Storage Seconds value is 864000, or 10 days.
9. In the Warning1Seconds field, enter the amount of time, in seconds, before the lease expiration date when the first notification of expiration is automatically sent to the server owner. The suggested Warning1Seconds value is 604800, or 7 days before lease expiration.
10. In the Warning2Seconds field, enter the amount of time, in seconds, before the lease expiration date when the second notification of expiration is automatically sent to the server owner. Depending on the width of your screen, you may need to scroll to the right to see the Warning2Seconds field. The suggested Warning2Seconds value is 86400, or 1 day before lease expiration.
11. Click **Save**.

Modifying a Lease Term Standard

Note that the Term label and the Runtime Seconds value **must** match. Do not modify either without modifying the other.

1. Choose **Setup > System Settings > Standards** tab.
2. Click **Define Order Standards**.
3. In the Standard panel on the left, move through the standards type to view settings.
4. Click **Lease Terms** in the Service Options folder on the left.
5. In the Standard Data column, click inside the Term field in the appropriate row and change the label (for example, 8 weeks). This entry will appear to users in the drop-down list on the order forms.

Note: It is recommended that you avoid using months, because the numbers of days in months vary. Because lease durations are defined in seconds, and the seconds values would not be consistent from month to month. It is recommended that you use four-week units instead of months.

6. Use the figures in the table above to calculate a duration in seconds.

Note: The runtime must match the number of seconds in the Term you have entered. Do not include commas in the value.

7. For Storage Seconds, Warning1Seconds, and Warning2Seconds, you can change the values, or accept the default values:

- Storage Seconds—864000 (10 days)
- Warning1Seconds—604800 (7 days)
- Warning2Seconds—86400 (1 day)

Note: Depending on the width of your screen, you may need to scroll to the right to see the Warning2Seconds field.

8. Click **Save**.

Deleting a Lease Term Standard

Do not delete or modify the No Lease standard unless you want to enforce leases on servers. If you delete the No Lease standard, users will not be able order servers without leases.

1. Choose **Setup > System Settings > Standards** tab.
2. Click **Define Order Standards**.
3. In the Standard panel on the left, move through the standards type to view settings.
4. Click **Lease Terms** in the Service Options folder on the left.
5. In the Standard Data column, click inside the Term field for the standard that you want to delete.
6. Click **Delete**, then confirm the deletion.
7. Click **Save**.

Adding, Modifying, or Deleting an Operating System Standard

Cisco IAC ships with five pre-defined O/S standards that users can choose when commissioning virtual machines with operating systems installed and administrators use to register VM templates:

- **Linux**–CentOS 5/6 64-bit
- **Linux**–Red Hat Enterprise Linux 6 64-bit
- **Windows**–Windows Server 2008 R2 64-bit
- **VMware ESXi**–ESXi 4.1
- **ESXi**–ESXi 5.0

Adding an Operating System Standard

1. Choose **Setup > System Settings > Standards** tab.
2. Click **Define Order Standards**.
3. In the Standard panel on the left, move through the standards type to view settings.
4. Click **OS Systems** in the Service Options folder on the left.
5. Click **Add New**. An empty row appears.
 - a. In the **Standard Data** column, click inside the **OS Type** field in the new row and enter the OS Type (Windows, Linux, or VMware ESXi). This entry will appear to users in drop-down lists on the order forms.
 - b. In the **OS System** field, enter the name of the operating system and the version number.
6. Click **Save**.

Modifying an Operating System Standard

1. Choose **Setup > System Settings > Standards** tab.
2. Click **Define Order Standards**.
3. In the Standard panel on the left, move through the standards type to view settings.
4. Click **OS Systems** in the Service Options folder on the left. In the Standard Data column, click inside the OS System field in the new row and edit the value.
5. Click **Save**.

Deleting an Operating System Standard

1. Choose **Setup > System Settings > Standards** tab.
2. Click **Define Order Standards**.
3. In the Standard panel on the left, move through the standards type to view settings.
4. Click **OS Systems** in the Service Options folder on the left. In the Standard Data column, click inside the OS System field for the standard that you want to delete.
5. Click **Delete**, then confirm the deletion.
6. Click **Save**.

Adding, Modifying, or Deleting a Server Size Standard

Cisco IAC ships with four predefined server size standards that users can choose when commissioning servers: Small, Medium, Large, and Extra Large. Each standard defines the CPU, Memory GB, and Storage GB.

Server Size	CPUs	Memory (GB)	Storage (GB)
Extra Small	1	1	30
Small	2	2	30
Medium	2	4	40
Large	4	6	40
Extra Large	8	8	60

You can accept, modify, or delete a server size standard, and you can add a new standard.

Note: For Order VM and Install OS the minimum disk size must be 30GB.

Adding a Server Size Standard

1. Choose **Setup > System Settings > Standards** tab.
2. Click **Define Order Standards**.
3. In the Standard panel on the left, move through the standards type to view settings.
4. Click **Server Size** in the Service Options folder on the left.
5. Click **Add New**. An empty row appears.
6. In the Standard Data column, click inside the Server Size field in the new row and enter the a label for the new size (for example, Extra Small). This entry will appear to users in drop-down lists on the order forms.
7. Enter the values for CPUs, Memory GB, and Storage GB in the appropriate fields.

Note: Depending on the width of your screen, you may need to scroll to the right to see the Storage GB field.

8. Click **Save**.

Modifying a Server Size Standard

1. Choose **Setup > System Settings > Standards** tab.
2. Click **Define Order Standards**.
3. In the Standard panel on the left, move through the standards type to view settings.
4. Click **Server Size** in the Service Options folder on the left.
5. In the Standard Data table, click in any of the fields to set new values.
6. Click **Save**.

Deleting a Server Size Standard

1. Choose **Setup > System Settings > Standards** tab.
2. Click **Define Order Standards**.
3. In the Standard panel on the left, move through the standards type to view settings.
4. Click **Server Size** in the Service Options folder on the left.
5. In the Standard Data column, click inside the Server Size field for the standard that you want to delete.
6. Click **Delete**, then confirm the deletion.
7. Click **Save**.

Adding, Modifying, or Deleting a VDC Size Standard

Cisco IAC ships with six predefined VDC standards that OTAs can choose when commissioning VDCs:

- Small, Medium, and Large standards define the sizes for VDCs.
- Small Shared, Medium Shared, and Large Shared standards define the sizes for Shared Zones.

Each standard defines the following settings:

Setting	Description
Maximum number of virtual servers limit	The maximum number of virtual servers allowed in this VDC. After this limit has been reached, additional virtual servers cannot be created in the VDC.
Maximum number of vCPU limit	The maximum number of vCPUs allowed in this VDC. After this limit has been reached, additional virtual servers cannot be created in the VDC
Maximum memory (GB) limit	The maximum amount of memory in GB allowed in this VDC. Enforcement of this limit is based on the memory specification in the Server standards. The memory limit is also used for creating the VMware resource pool.
Maximum total storage (GB) limit	The maximum amount of memory in GB allowed in this VDC. Enforcement of this limit is based on the storage specification in the Server standards. It does not account for thin provisioning or space used by snapshots.
Maximum number of physical servers limit	The maximum number of virtual servers allowed in this VDC. After this limit has been reached, additional virtual servers cannot be created in the VDC.
CPU Limit (MHz)	The maximum amount of CPU in MHz virtual servers in this VDC is allowed to use. This number is determined by the CPU compute capacity available in the cluster. This enforced through the VMware resource pool CPU Limit. -1 specifies unlimited.
Resource Pool CPU Reservation (MHz)	The amount of CPU in MHz to reserve for this VDC. The reservation is handled by the VMware resource pool CPU Reservation. The default is 0.
Resource Pool Memory Reservation (GB)	The amount of memory in GB to reserve for this VDC. The reservation is handled by the VMware resource pool Memory Reservation. The default is 0.
Number of Snapshots	Default value for maximum number of snapshots allowed per VDC. After this limit has been reached for a virtual server, no additional snapshots can be taken for that server.
Community VDC (Yes - No boolean)	Specifies whether this standard applies to a Shared Zone Community VDC. This should be set to Yes , if this standard is for a Shared Zone Community VDC and No , if this standard is for an organization VDC. This setting is case sensitive.
Size Order	Specifies the order of the sizes relative to each other. An Integer is used to define this. For example, Small is 1, Medium is 2, Large is 3.

Adding, Modifying, or Deleting a VDC Size Standard

The following table summarizes the maximum values for the virtual servers. You can accept, modify, or delete a server size standard, or you can add a new standard. To add a new standard, use the VDC Size Calculator determine the proper VDC sizing. For more information about the VDC Calculator, see [Planning VDC Package Sizing, page 160](#).

Table 1 Maximum Values for Virtual Servers

	Max Virtual Servers	Max vCPU	Max Memory (GB)	Max Total Storage (GB)	Max Physical Servers	CPU Limit (MHz)	Resource Pool CPU Reservation (MHz)	Resource Pool Memory Reservation (GB)	Number of Snapshots	Community VDC
Small	50	74	296	7500	0	22,200	0	0	5	No
Medium	100	145	580	14,750	2	43,500	0	0	5	No
Large	250	366	1458	37,002	4	109,200	0	0	5	No
Small Shared	250	366	1458	37,002	10	109,200	0	0	5	Yes
Medium Shared	500	725	2900	73,750	10	217,500	0	0	5	Yes
Large Shared	1000	1450	5800	147,500	10	435,000	0	0	5	Yes

Adding a VDC Size Standard

Use the VDC calculator to calculate the appropriate values for the number of virtual servers for this standard (choose **Setup > VDC Calculator**).

1. Choose **Setup > System Settings > Standards** tab.
2. Click **Define Order Standards**.
3. Click **VDC Sizes** in the Virtual Data Center folder on the left.
4. Click **Add New**. An empty row appears.
5. In the Standard Data column, click inside the Name field in the new row and enter the a label for the new size (for example, Extra Small). This entry will appear to users in drop-down lists on the order forms.
6. Enter the values for the other fields based on the results provided by the VDC Size calculator. Depending on the width of your screen, you may need to scroll to the right to see the Storage GB field.
7. Enter **Yes** if this standard is a shared zone community VDC or **No** if this standard is for a organization VDC.
8. For the **Size Order**, specify an integer for the new standards size relative to the other sizes. For example, **1** for Small.
9. Click **Save**.

Modifying a VDC Size Standard

1. Choose **Setup > System Settings > Standards** tab.
2. Click **Define Order Standards**.
3. Click **VDC Sizes** in the Virtual Data Center folder on the left.
4. In the Standard Data table, click in any of the fields to set new values.
5. Click **Save**.

Deleting a VDC Size Standard

1. Choose **Setup > System Settings > Standards** tab.
2. Click **Define Order Standards**.
3. Click **VDC Sizes** in the Virtual Data Center folder on the left.
4. In the Standard Data table, click inside the Name field for the standard that you want to delete.
5. Click **Delete**, then confirm the deletion.
6. Click **Save**.

Planning VDC Package Sizing

Only Cloud Provider Technical Administrators have access to this feature. Cloud Provider Technical Administrators often need to determine the most effective sizes for virtual data center packages to match their customer's needs.

To avoid any big leftover gaps or unused resources, the VDC Calculator can help build well-balanced offerings that closely match a customer needs, with the correct ratios between size elements of the package (CPU, memory, and storage resource limitations).

1. Choose **Service Portal** from the module drop-down list.
2. Click the **VDC Calculator** tab.
3. In the Planned VDC VM Limit step, enter the approximate number of virtual machines in the VDC.
4. In the **Planned VM Distribution** step, enter names for each virtual machine size and the respective virtual machine percentages. For readability, try to make the distribution percentage equal to 100%.
5. The **Planned VM Configuration** step displays the respective virtual machine configuration attributes for each size. The VDC Calculator uses these attributes, plus the following values, to create a weighted average:
 - **MHz allocated per vCPU**—Enter how much real CPU (in MHz) should be assumed per vCPU allocated to a VM. This drives the total MHz boundaries of the resource pool.
 - **Snapshots per VM**—Enter how many snapshots will be assumed when calculating the suggested datastore size.
6. The VDC Calculator returns the suggested VDC package.



Exporting Data

You can export a file containing data from all rows and columns (displayed or not) in the tables listed below for Cisco Intelligent Automation for Cloud 4.1. The file is a CSV (comma delimited text file), compatible with Microsoft Office and OpenOffice, as well as most data analysis programs.

List of Tables With Export Functionality

- **Order Status**
- **My Servers**
- **My VDCs**
- **My Run Rate**
- **Error Remediation**
- **Network Management**
- **Manage Infrastructure**
- **VMware vCenter Server**
 - Virtual Machines
 - VM Templates
 - Portgroups
 - Resource Pools
 - Datastores
 - Hosts
 - Clusters
 - Data Centers
- **VMWare vCloud Director**
 - vApp Templates
 - External Networks
 - Organization Networks
 - Organization VDCs
 - Organizations
 - Provider VDCs

List of Tables With Export Functionality

- VM Templates
- **OpenStack**
 - Flavors
 - Floating IP Pools
 - Images
 - Keypairs
 - Volumes
 - Projects
 - Security Groups
- **Network Elements**
 - Network Devices
 - Citrix NetScaler 1000v
 - Nexus 1000V
- **Cisco Prime Network Services Controller**
 - Cisco ASA 1000v
 - Cisco VSG
 - Cisco CSR 1000V
- **Cisco UCS Manager**
 - UCS Blades
 - UCS Rack Servers
 - UCS vLans
 - UCS vNIC Templates
 - Service Profile Templates
- **Cisco UCS Director**
 - Physical Accounts
 - Virtual Accounts
 - Catalogs
 - VMware Computing Policies
 - VMware Network Policies
 - VMware Storage Policies
 - VMware System Policies
 - Hyper-V Computing Policies

Exporting a Data File

- Hyper-V Network Policies
- Hyper-V Storage Policies
- Hyper-V Deployment Policies
- **Amazon EC2**
 - Images
 - Instance Types
 - Key Pairs
 - Networks
 - Security Groups
- **Cisco IAC Management Appliance**
 - Images
- **Chef**
 - Chef Roles
 - Chef Cookbooks
 - Chef Environments
 - Chef Databags
- **Puppet**
 - Puppet Roles
 - Puppet Profiles
 - Puppet Environments
 - Puppet Modules

Exporting a Data File

To export a CSV data file from any of the tables listed above, simply click the Export icon or button located on the form from which you want to export the data. A .csv is downloaded immediately to your default download location. (Typically, you will see the file listed in your browser's download listings area.)

