Cisco Intelligent Automation for Cloud User Guide

Release 3.1.1
Published: February 1, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-28883-01

Cisco Intelligent Automation for Cloud 3.1.1 User Guide

CONTENTS

Preface

The Cisco Intelligent Automation for Cloud 3.1.1 User Guide provides instructions for setting up, managing, and ordering from the Cloud Portal. This user guide provides documentation for both the full version of Cisco Intelligent Automation for Cloud and Cisco Intelligent Automation for Cloud Starter Edition.

About Cisco Intelligent Automation for Cloud 3.1.1

Cisco Intelligent Automation for Cloud is a cloud management software solution that delivers a critical foundation layer for deploying and managing cloud-based computing in a holistic and unified way. The solution provides essential automated management and orchestration that allows organizations to control and manage cloud-based services transparently throughout their lifecycles. This solution can cover diverse cloud deployments and is a flexible solution that can scale from test and development to production workloads, from initial cloud pilots to large-scale enterprise-wide initiatives to deliver maximum value to customers.

Cisco IAC includes the following products to provide cloud compute and cloud orchestration:

- Cisco Cloud Portal—Provides the self-service portal from which employees of the organization can order services
- Cisco Process Orchestrator—Provides the orchestration and reporting for services ordered through Cloud Portal
- Cisco Server Provisioner—Performs network based provisioning on physical or virtual servers

Cisco Intelligent Automation for Cloud Licensing

Intelligent Automation for Cloud customers who purchased or are upgrading from versions 2.0, 3.0 Starter Edition, 3.0.1 Starter Edition, or 3.0.2 Starter Edition must request a new license code in order to run the new IAC 3.1.1 content and get full access to new features. Without this new license code, IAC will fail to execute correctly since IAC content depends on the new Cisco Service Portal adapter in Cisco Process Orchestrator. Customers who purchased and are upgrading from IAC 3.1 do not need to obtain a new key, since the IAC 3.1 license key enabled all of the new elements.

When IAC 2.0 customers upgrade to IAC 3.1, they will be entitled to the following Process Orchestrator adapters:

- Cisco Network Services Manager
- Cisco Service Portal

- VMware vCloud Director.

Customers who purchased an IAC Starter Edition version are entitled to the Cisco Service Portal adapter, but are not entitled to the Cisco Network Services Manager and VMware vCloud Director adapters. To gain entitlement to these items, customers need to purchase an upgrade from Starter Edition to Intelligent Automation for Cloud.

When an order is placed, the customer receives a claim certificate. The claim certificate provides the product authorization keys (PAK) and a link to the Cisco Product License Registration portal where the customer must register the PAK keys. When the keys are registered, the licensing team issues the keys to the customer.

For the upgrade to IAC 3.1.1, the customer should contact TAC and will be referred to GLO (Global Licensing Organization) to request a new license code. The request should reference the original PAK key, the need for a new license code for Cisco Intelligent Automation for Cloud, and the host name on which Cisco Process Orchestrator will be installed.

Once the customer receives the new license code, it can be entered in Cisco Process Orchestrator 2.3.5's administration screens.

Differences between Cisco Intelligent Automation for Cloud Editions

Table i-1 Cisco IAC Version Comparison

	Cisco IAC SE 3.1.1	Cisco IAC 3.1.1 (full version)
Maximum NSM connections	Zero	Unlimited
Maximum UCS connections	One	Unlimited
Maximum PODs	One	Unlimited
Maximum VDCs per organization	One	Unlimited

There are several differences between Cisco IAC SE 3.1.1 and Cisco IAC 3.1.1:

In Cisco IAC SE 3.1.1:

- The shared zone does not have resource pools or datastores associated with it; it contains community networks, platform elements, and a single data center.
- An organization has one datastore, one resource pool, and zero or more networks assigned to it.
- Organization units have a flat structure. The cloud administration organization and non-cloud administration organizations are flat in structure.
- Virtual servers are provisioned in the organization's datastore and resource pool. The virtual server can be provisioned to either an organization-specific network or community network.

In Cisco IAC 3.1.1:

- A Point-of-Delivery (POD) contains the platform elements and a data center. Multiple data centers are supported through multiple Compute PODs.
- The Shared Zone is assigned one resource pool, one datastore, and one or more community networks. Multiple Shared Zones may be created.
- A virtual data center is assigned one resource pool, one datastore, and one or more user networks. Multiple virtual data centers may be created and assigned to an organization.
- Virtual servers can be provisioned either in the virtual data center or in the shared zone.

- Community networks are only accessible via a shared zone.

How to Upgrade from Cisco IAC SE to the Full Version of Cisco IAC

Cisco IAC licensing is done through Cisco Process Orchestrator. When you receive the license key for the full version of Cisco IAC, follow these steps in Process Orchestrator:

Step 1 The Update License Wizard is used to update your license. From the **File** menu, select **Update**. The License Information panel displays.

Step 2 In the following fields, enter the appropriate information and click **Next**. The License Agreement panel displays.

Field	Description
Customer name	Name of the individual client or department
Company name	Enter the name of your company exactly as provided by Cisco Systems. This field is case-sensitive.
License code	Enter the license code exactly as provided by Cisco Systems.

Step 3 Choose the **I agree** radio button and click **Next**. The Completing the Update License Wizard panel displays.

Step 4 Review the information and click **Finish**. A confirmation message dialog box displays that the license update was successful.

Step 5 Click **OK** to complete the procedure.

Step 6 The Process Orchestrator console displays.

Step 7 Licensing is refreshed periodically at one-hour intervals in Process Orchestrator; if you have an immediate need, you may follow the next steps to manually refresh the license.

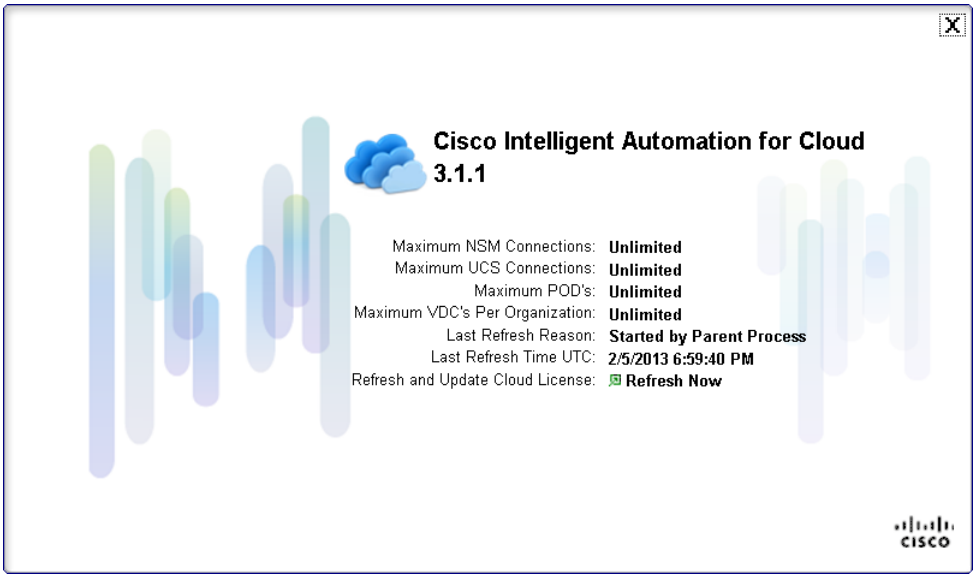
Step 8 In Cisco IAC, follow the steps in How to View the Cisco IAC/Cisco IAC SE About Popup, page x then follow the steps in How to Manually Refresh the Cisco IAC/Cisco IAC SE License, page x.

How to View the Cisco IAC/Cisco IAC SE About Popup

Note Only Cloud Provider Technical Administrators have permissions to access the Cisco IAC/Cisco IAC SE About popup.

To view the Cisco IAC/Cisco IAC SE About popup, click the Copyright link on the bottom right of the My Workspace Site Homepage (Welcome screen).

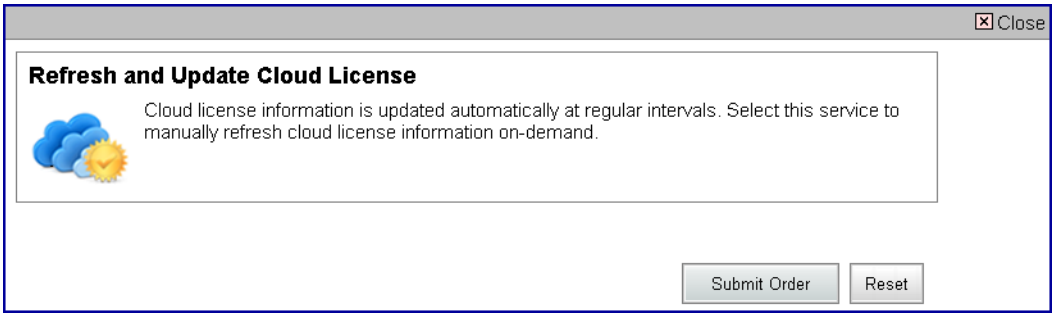
Figure i-1 Cisco IAC/Cisco IAC SE About Popup



How to Manually Refresh the Cisco IAC/Cisco IAC SE License

Step 1 To manually refresh the Cisco IAC/Cisco IAC SE license, go to the About popup (see How to View the Cisco IAC/Cisco IAC SE About Popup, page x) and click **Refresh Now**.

Figure i-2 Refresh and Update Cloud License screen



Step 2 Click **Submit Order**.

Organization

This guide includes the following sections:

Chapter 1	Introduction	Introduces Cisco Intelligent Automation for Cloud, describes user roles, and provides information about navigating the Cloud Portal.
Chapter 2	Ordering Cloud Services	Provides steps for all users for ordering physical and virtual servers.
Chapter 3	Managing the Cloud System	Guides Cloud Provider Technical Administrators and Organization Technical Administrators through lifecycle of servers and networks.
Chapter 4	Managing Organizations and Users	Guides Cloud Provider Technical Administrators and Organization Technical Administrators through managing organizations and end-users.
Chapter 5	Managing Services	Guides Cloud Provider Technical Administrators through tracking service requisitions, setting standards for service items, managing server leases, and handling Cloud infrastructure errors.

Conventions

This guide uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem*.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning **Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.**

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

In addition to this document, the following guides have been updated for Cisco IAC:

- *Cisco Intelligent Automation for Cloud 3.1.1 Compatibility Matrix*
- *Cisco Intelligent Automation for Cloud 3.1.1 Configuration Guide*
- *Cisco Intelligent Automation for Cloud 3.1.1 Release Notes*

You can access the most current Cisco IAC documentation, including these release notes, online at [http://www.cisco.com/en/US/products/ps11869/tsd_products_support_series_home.html].

Documentation Formats

Documentation is provided in the following electronic formats:

- Adobe® Acrobat® PDF files
- Online help

You must have Adobe Reader® installed to read the PDF files. Adobe Reader installation programs for common operating systems are available for free download from the Adobe website at www.adobe.com.

Online Help

Online help is available for Cisco Process Orchestrator and Cisco Cloud Portal.

For Process Orchestrator, you can access online help using the following methods:

- Click the **Help** button on any dialog in the application to open the help topic in a pane to the right of the dialog.
- In the Process Orchestrator console:
  - Click the **Help Pane**  tool on the toolbar to open the help topic in a pane to the right of the console results pane.
  - Click **Help** on the menu bar.

For Cisco Cloud Portal, access online help by clicking the question mark icon in the upper right corner of the window.

Product Naming Conventions

The following product naming conventions are used throughout this document and in the Cisco IAC user interface:

- Cisco Tidal Enterprise Orchestrator, TEO, and Process Orchestrator are synonymous with Cisco Process Orchestrator.
- Cisco Service Portal is synonymous with Cisco Cloud Portal.

Other Naming Conventions

Cloud Administrator is synonymous with **Cloud Provider Technical Administrator**.

Open Source License Acknowledgements

Licenses and notices for open source software used in Cisco Process Orchestrator can be found in the Open Source License Acknowledgements found on Cisco.com. If you have any questions about the open source contained in this product, please email external-opensource-requests@cisco.com.

CHAPTER 1

Introduction

Cisco Intelligent Automation for Cloud 3.1.1 (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 Cisco Cloud Portal, a browser-based interface that provides links to services and status, such as ordering servers, viewing requisitions, monitoring system resources.

This section introduces you to the Cloud Portal, organizations, service teams, and user roles. It includes the following sections:

Cloud Portal is a browser-based set of applications that organizations and service teams log into and orders and manages services.

Understanding Organizations

In the Cloud Portal environment, organizations are users who are grouped according to function or business. There are two kinds of organizations: business units and service teams.

Business Units

Business units 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 1-18)
- Virtual Server Owner (Virtual Server Owner, page 1-18)
- Virtual and Physical Server Owner (Virtual and Physical Server Owner, page 1-18)

Service Teams

Service teams are units whose members administer and maintain the Cisco IAC solution, which includes Cloud Portal. 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. For information on the Cloud Provider Technical Administrator role, see Cloud Provider Technical Administrator, page 1-17)

Navigating Cloud Portal

Note Your level of access to services and modules depends on your user role in Cloud Portal.

Modules

Modules are role-based containers of Cloud Portal services grouped by purpose. This section describes Cloud Portal modules containing services that are covered in this guide.

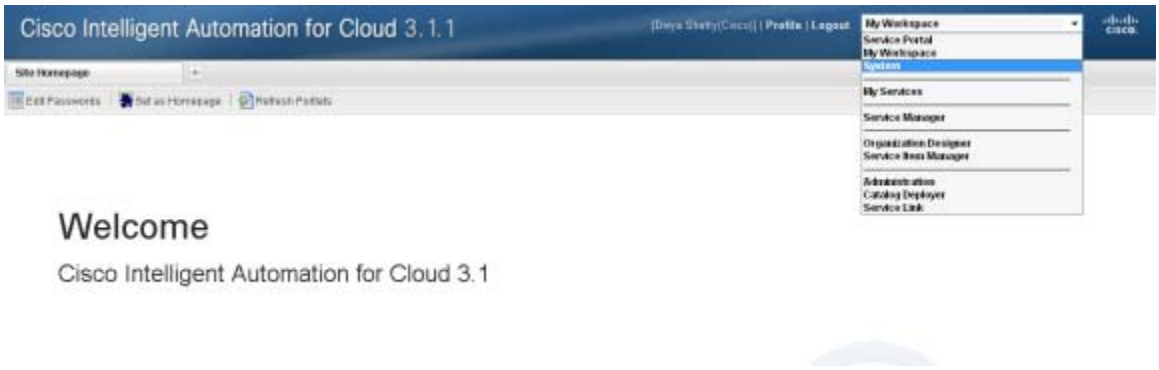
- Organization Designer, page 1-7
- Service Item Manager, page 1-8
- Administration, page 1-9

Note The Portal Designer, Service Designer, Catalog Deployer, and Service Link modules are used by Site Administrators to set up and maintain the Cloud Portal environment. These modules contain services that could alter or corrupt your environment settings if executed. It is strongly recommended that you do not use these services. It is also recommended that you do not use services that are accessible in Cloud Portal but not covered in this guide.

Accessing Modules

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.

Figure 1-1 Module Drop-down List

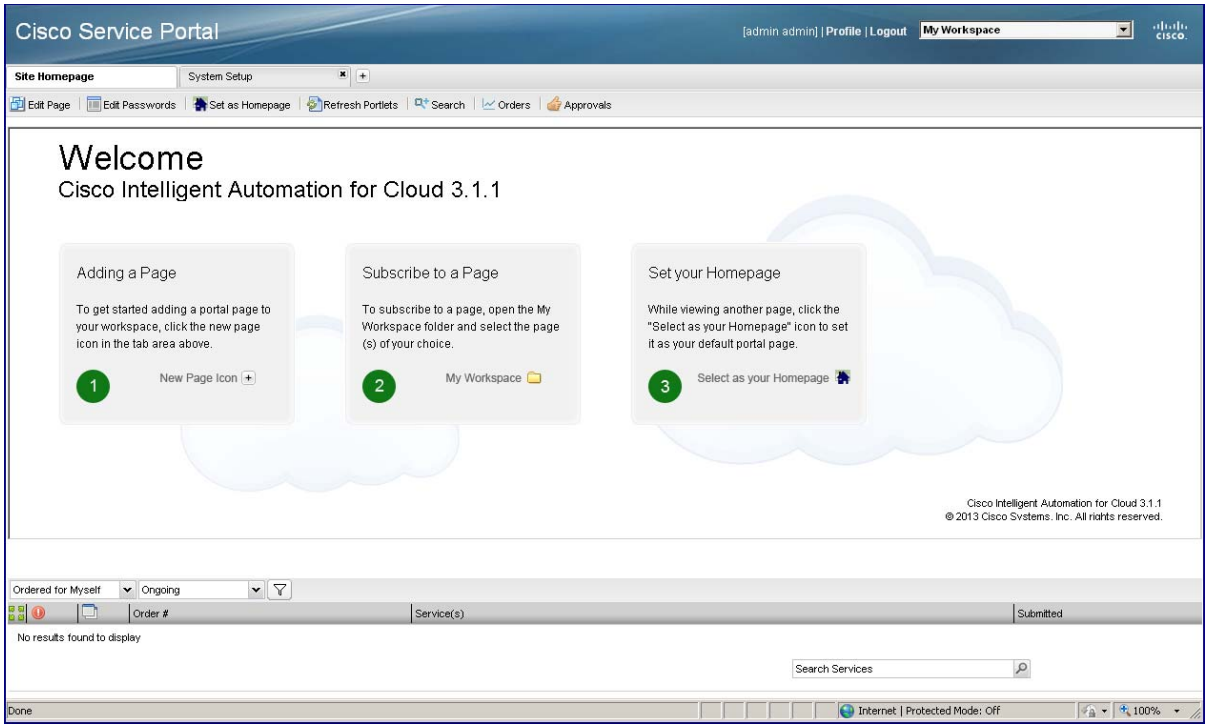


Site Homepage/My Workspace

The Site Homepage is by default your Cloud Portal login landing page. Also known as **My Workspace**, it provides easy access to the portal pages and portlets, where you can perform the most common tasks, including ordering servers and configuring networks. You can also edit your profile preferences and subscribe to pages from the Site Homepage.

Note In some cases when you first log in, your landing page is My Services instead of My Workspace. See Changing Your Landing Page from My Services to My Workspace, page 1-5 to correct this problem.

Figure 1-2 Site Homepage/My Workspace



Access the Site Homepage by choosing **My Workspace** from the module drop-down list on the upper-right corner of the screen.

Note You can change your login landing page to another module. For instructions, see Adding Portal and Portlet Access to My Workspace, page 1-12.

To access portal pages, you must add tabs to the My Workspace module page. For instructions, see the following section, Adding Portal Page Access to My Workspace.

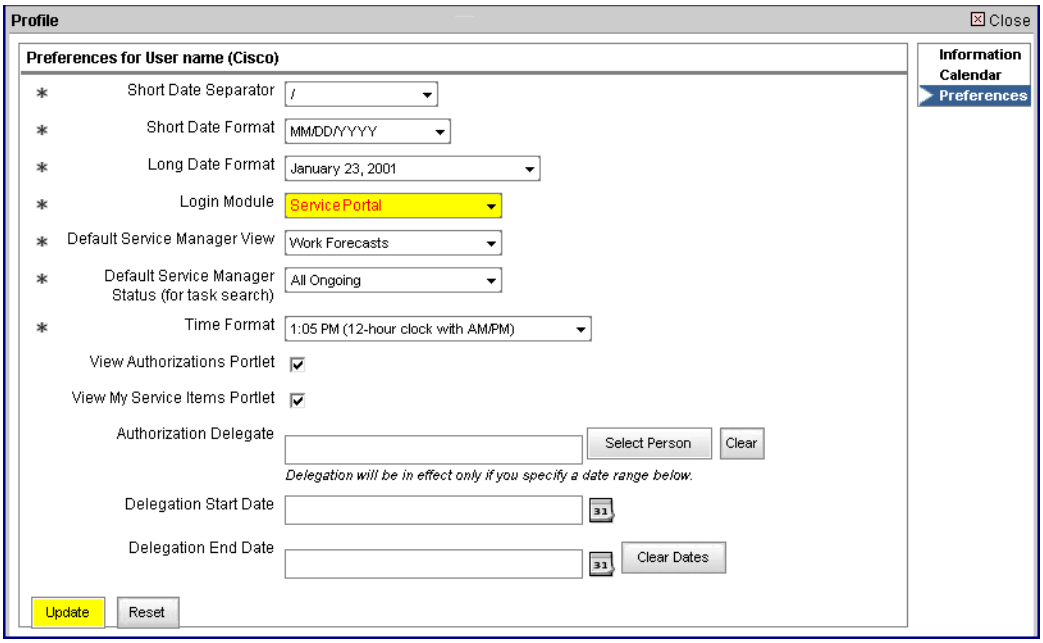
Changing Your Landing Page from My Services to My Workspace

In some cases when you first log in, your landing page is My Services instead of My Workspace. Follow these steps to correct this issue.

Step 1 Click **My Profile** next to the module drop-down list in the upper-right corner of the window. Cloud Portal displays the Information screen of your profile.

Step 2 Click **Preferences** in the upper-right corner of the Information screen. Cloud Portal displays the Preferences screen of your profile.

Figure 1-3 Preferences screen of your profile



Step 3 With the **Login Module** drop-down list, choose **Service Portal**.

Step 4 Click **Update**.

Adding Portal Page Access to My Workspace

To order most Cloud Portal services, you must have access to portal pages in My Workspace in the form of tabs. If you do not already have access to the portals, use to following steps to add them.

For more information on portals, see Portals and Portlets, page 1-9.

Step 1 Open Cloud Portal in your browser and log in to the application.

Step 2 Choose the **My Workspace** from the module drop-down list.

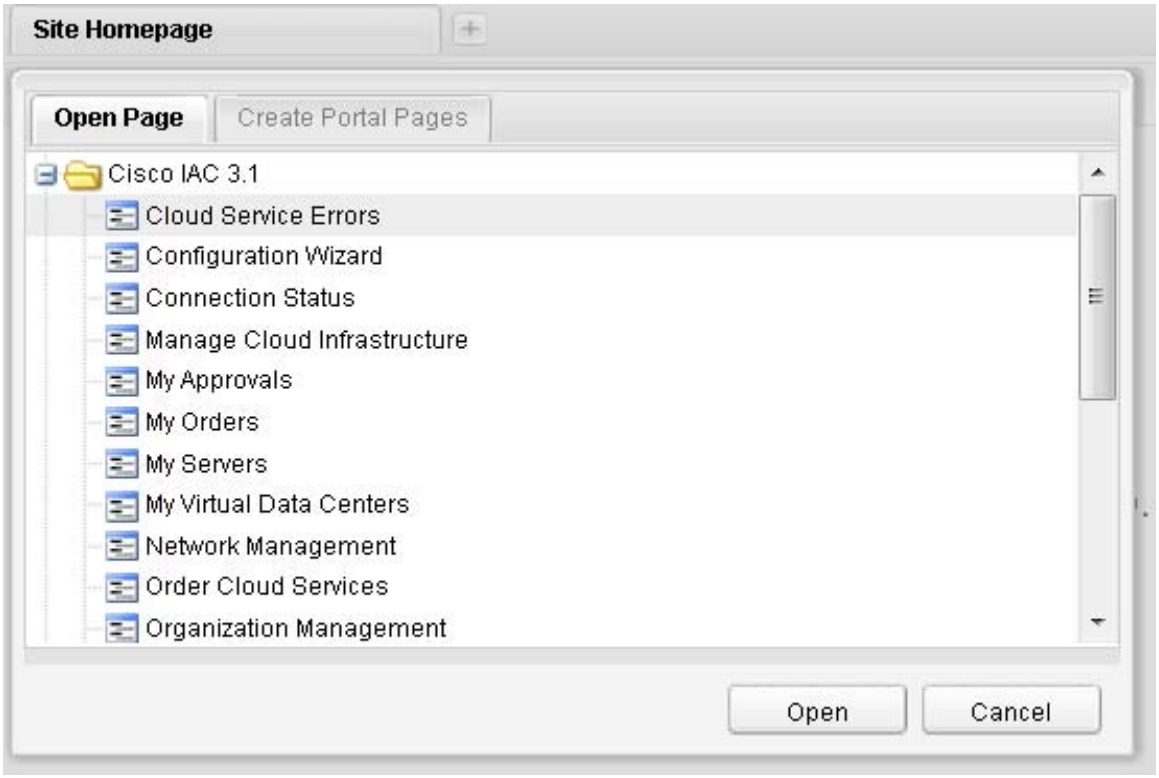
Step 3 On the page, click the + to open the Open Page dialog box.

Figure 1-4 Adding Portals to My Workspace

Step 4 Expand the **Cisco IAC 3.1** folder.

Step 5 Click to select a portal page, then click **Open** to create a tab for the portal.

Figure 1-5 Open Page



Note The portals shown in Figure 1-5 are not available to all users.

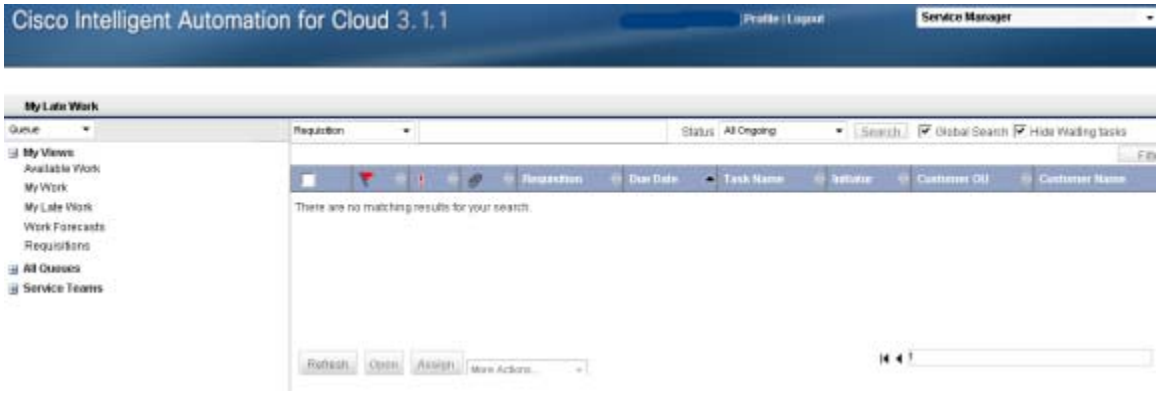
Step 6 Repeat Step 3 through Step 5 for each portal in the **Cisco IAC 3.1** and **My Workspace** folders.

Service Manager

Note Cloud Provider Technical Administrators, Organization Technical Administrators, and site administrators have permissions to access the Service Manager module.

Service Manager enables Cloud Provider Technical Administrators to manage, assign, and track progress on tasks for Service Team members. The Cloud Provider Technical Administrator uses ERS and Approvals portlets to try and remediate Cloud services.

Figure 1-6 Service Manager Module



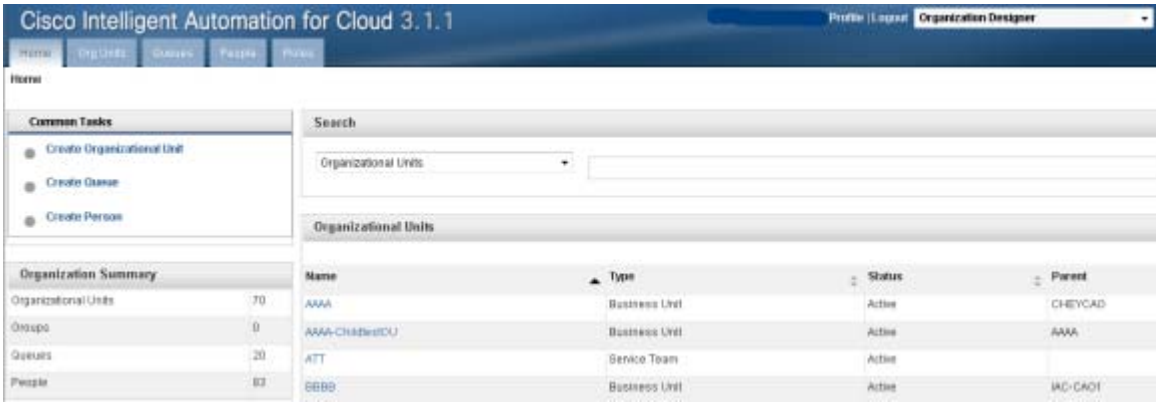
Organization Designer

Note Cloud Provider Technical Administrators and site administrators have permissions to access the Organization Designer module.

Cloud Provider Technical Administrators use Organization Designer to create, modify, and remove users.

Note Organizations can only be modified in the Organization Management portal. See Site Homepage/My Workspace, page 1-4 for how to access portal pages; see Chapter 4, "Managing Organizations and Users" for information on modifying an organization.

Figure 1-7 Organization Designer Module Home Page



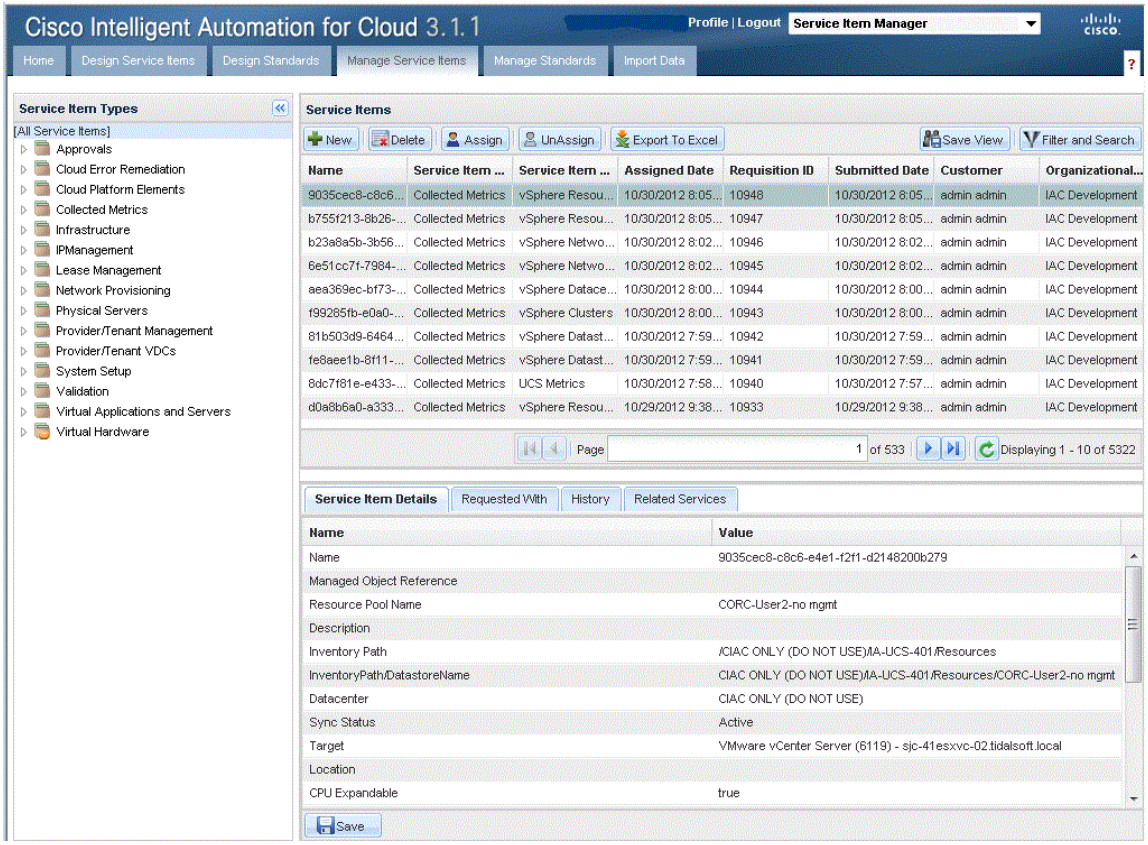
Service Item Manager

Note Only Cloud Provider Technical Administrators and site administrators have permissions to access the 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 that users can order; these options appear in drop-down lists on server order forms.

Figure 1-8 Service Item Manager Module—Manage Service Items Tab



Administration

Note Only Cloud Provider Technical Administrators have permissions to access the Administration module.

Access the Administration module to perform administrative tasks, such as editing system-wide settings and configuring authorizations and reviews.

Portals and Portlets

Portal pages and portlets (subsets of certain portals) contain links to the order forms for services.

Portals

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

- Provide information—For example, the System Resources 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 (virtual machines only).

Cisco IAC provides the following portal pages. Access depends on your role.

- Cloud Service Errors—Access to the Cloud Service Errors, which contains the service links to Error Remediations services such as Cancel, Restart, Retry, Ignore and Rollback.
- 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.
- Manage Cloud Infrastructure—Access to Discovery and Manage Cloud Infrastructures.
- My Approvals—Displays approvals asssigned to you directly or to your queues, and enables you to see approvals that preced or follow yours. Depending on your role, you may also be able to see approvals for orders placed by user in your business units.
- 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 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 Virtual Data Centers—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 and Order a Physical Server.
- Network Management—View network IP addresses and network capacity information. Only Cloud Provider Technical Administrators can access the Network Management portal page.
- Order Cloud Services—Commission a virtual or physical server. All users can access the Order Cloud Services portal page.
- Organization Management—Add, modify, and remove organizations, and add or remove an organization network. Both Cloud Provider Technical Administrators and Organization Technical Administrators can access the Organization Management portal page.
- POD Resource Capacity—Displays the status of PODS.
- System Health—Aaccess to the System Health details, which contains the service links to validate the Platform Elements, validate Cisco Process Orchestrator and Validate Email Server..
- System Resource Capacity—View capacity information for virtual clusters, UCS blades, and chassis. Only Cloud Provider Technical Administrators can access the System Resources portal page.
- System Resource Usage—Displays the status of UCS Physical Blade Pool Management.

- System Setup—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.
- Upgrade Wizard—Perform the steps in this wizard to upgrade Intelligent Automation for Cloud.
- User Management—Add, modify, or remove users in an organization. Both Cloud Provider Technical Administrators and Organization Technical Administrators can access the User Management portal page.
- VDC Calculator—Calculate the Planned VM Distribution, Planned VM Configuration and Suggested VDC Package from Planned VDC VM Limit.

Portlets

Note Only Cloud Provider Technical Administrators can access the portlets.

Portlets are subcategories of the System Setup portal page in My Workspace.

The System Setup portal page contains the portal tabs:

Portlet	Tasks
Administrators	• Create the Cloud Provider Technical Administrator Organization • Add a Cloud Provider Technical Administrator • Remove a Cloud Provider Technical Administrator
Connections	• Connect or update connections of three platform elements: – VMware vCenter Server – Cisco UCS Manager – Cisco Server Provisioner • Set up or modify directory integration information for the following: – Datasources – Mappings – Events
PODs	• Register a POD • Remove a POD • Modify POD properties
Blades and Pools	• Register or remove Cisco UCS blades • Manage blade pools
System Settings	• Modify REX agent or HTTP agent configuration • Set provisioning settings • Modify email notification templates
Networks	• Add or remove networks • Modify properties of networks
Shared Zone	• Update the shared server zone

Portlet	Tasks
Standards	Modify or create order standards for services
Approvals	Configure approvals
About	Displays the About portlet

Managing My Workspace

Adding Portal and Portlet Access to My Workspace

Add access, in the form of tabs, to the portals and portlets in My Workspace.

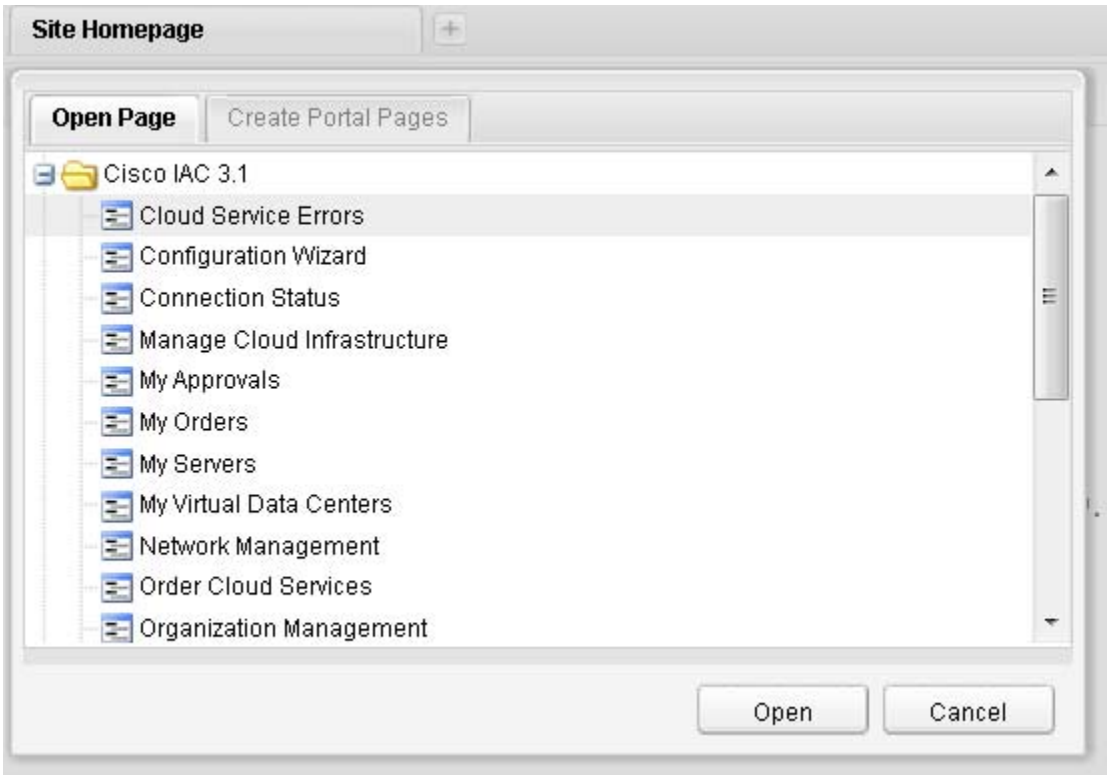
Note Cloud Portal ships with reserved portlets for searching, tracking orders, and approvals. The portlets can be added to individual portals in My Workspace by clicking buttons on the toolbar. The reserved portlet buttons appear by default. If a user adds a reserved portlet to a portal, it cannot be removed or edited. However, you can hide the reserved portlet buttons from the toolbar. For instructions on removing the buttons, see Removing Reserved Portlet Buttons from the My Workspace Toolbar, page 1-13.

Step 1 Open Cloud Portal and log in to the application as an administrator.

Step 2 Choose the **My Workspace** from the module drop-down list.

Step 3 Click **+** to display the **Open Page** dialog box.

Figure 1-9 My Workspace—Open Page Dialog Box



Step 4 Expand the **Cisco IAC 3.1** folder.

Step 5 Select a portlet and click **Open** to add a tab for the portlet.

Step 6 Click **+** to expand the Open Page dialog box.

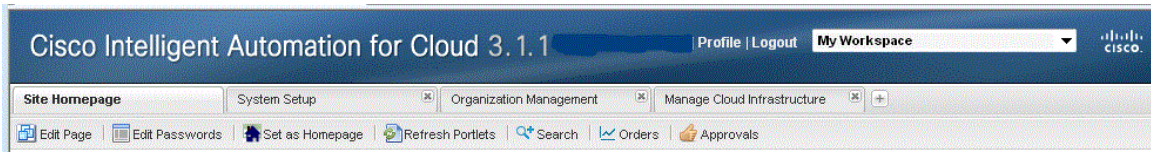
Step 7 Repeat Step 5 for each portlet in the IAC folder.

Step 8 Expand the **My Workspace** folder, and repeat Step 5 for the **My Servers** and **Order Cloud Services** portlets.

Removing Reserved Portlet Buttons from the My Workspace Toolbar

Reserved portlets are out-of-the-box portlets that ship with Cisco Cloud Portal. Reserved portlets can be added to portals by clicking buttons in the toolbar in the My Workspace module. Unless you hide them, these buttons appear by default.

Figure 1-10 My Workspace—Reserved Portlet Buttons

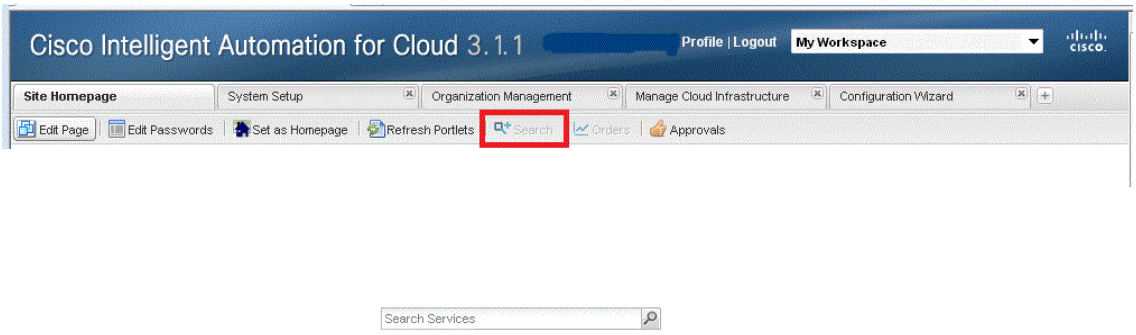


There are three reserved portlets:

Reserved Portlet Button	Description
Search	Adds a Search portlet to the current portal. It allows you to search for services by service 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, as shown in Figure 1-11 on page 1-14.

Figure 1-11 My Workspace—Search Portlet



Reserved portlets cannot be removed from a portal or edited once they are 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.

Step 1 Choose **Portal Designer** from the module drop-down list, then click the **Portlets** tab.

Step 2 Expand **Reserved Portlets** in the left pane and click any of the portlets in the folder.

Step 3 In the Content Portlet Information pane, click the **Inactive** radio button.

Step 4 Click **Save**.

Step 5 Repeat Step 1 through Step 4 for other reserved portlets that you want to inactivate.

Note To reactivate a reserved portlets, follow Step 1 through Step 2, click the **Active** radio button, then click **Save**.

Profile Settings and Preferences

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

- Change your Cloud Portal 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

Note Changes to your personal settings, such as password and time zone, automatically update your Cloud Portal user account.

To access your profile settings, click Profile at the top of any page in Cloud Portal.

Customizing Table Views

In Cloud Portal, most table views are customizable for each 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 to meet your needs and make the information easier to read.

When you change the table view, your personal settings are retained unless or until you change them again, of if you have cookies disabled in your browser settings.

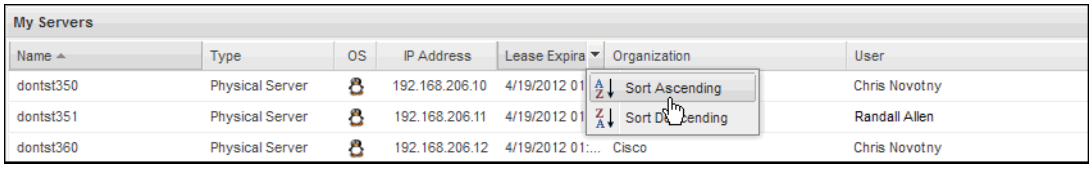
- Re-sorting Table Rows by Column, page 1-15
- Adding or Removing Columns, page 1-16

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**.

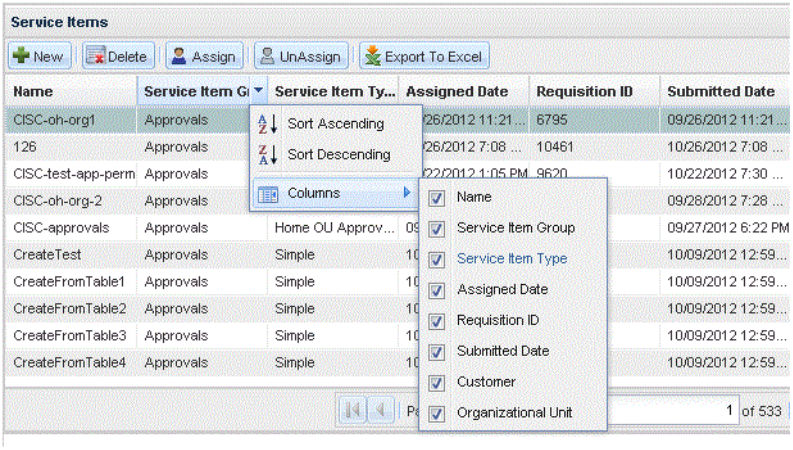
Figure 1-12 Sort Ascending by Column



Adding or Removing Columns

Hover the mouse pointer over the far right side of the column title until an arrow appears, click the arrow and choose **Columns**. In the Columns menu, check or uncheck the check boxes of any of the available columns.

Figure 1-13 My Servers—Adding or Removing Columns



User Roles and Capabilities

Cisco Intelligent Automation for Cloud features pre-defined user roles that determine what individuals can access and perform. There are several roles:

- Cloud Provider Technical Administrator, page 1-17
- Organization Technical Administrator, page 1-18
- Virtual Server Owner, page 1-18
- Virtual and Physical Server Owner, page 1-18
- Solutions Team, page 1-19
- Form Extender, page 1-19

Note User Roles and Capabilities, page 1-17 compares capabilities by role.

Additionally, the system-defined "Anyone" role includes all of the Cloud Portal 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.

Cloud Provider Technical Administrator

Cloud Provider Technical Administrators manage the underlying infrastructure of Cisco IAC—the Cisco Process Orchestrator, Cisco UCS Manager, Cisco Server Provisioner, VMware vCenter, and Cloud Portal. 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:

- Site Homepage/My Workspace, page 1-4—Access and perform tasks from all portals and portlets.
- Organization Designer, page 1-7—Create organizations and users.
- Service Manager, page 1-7
  - Track ordered service items charged to a particular department within an organization.
  - 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, page 1-8
  - Create or modify ordering standards such as available server sizes and managed lease term limits.
- Administration, page 1-9
  - Link to and utilize data from your enterprise directory and other sources of user data.
  - Customize your Cloud Portal 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.

Organization Technical Administrator

Organization Technical Administrators are employees 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 Cisco Cloud Portal. They also assign users to Server Owner roles within the organization.

The Organization Technical Provider has access to the following modules:

- Site Homepage/My Workspace, page 1-4—Access portals the following portals to order Cloud Portal services:
  - My Servers, page 1-10—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, page 1-11—Add, modify, and remove users.
  - Order Cloud Services, page 1-10—Commission a virtual machine.
- **My Services**—Create users and update user profile information

Virtual Server Owner

The Virtual Server Owner is an employee of the organization who orders and provisions virtual machines.

The Virtual Server Owner has access to the following portals in the My Workspace module (page 1-4):

- **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.

Virtual and Physical Server Owner

The Virtual and Physical Server Owner 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 My Workspace module (page 1-4):

- My Servers, page 1-10—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, page 1-10—Commission or decommission a virtual or physical server.

Solutions Team

The Solutions Team 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—
  - 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 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

Table 1-1 Capabilities by User Role

Category	Service	VSO[1]	V/PSO[2]	OTA[3]	CPTA[4]
Agents	Configure HTTPS agents	—	—	—	•
	Configure REX agents	—	—	—	•
Cisco UCS Blades	Register a Cisco UCS blade	—	—	—	•
	Manage blade pools	—	—	—	•
	Remove a Cisco UCS blade	—	—	—	•
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	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	—	—	—	•

Table 1-1 Capabilities by User Role

Category	Service	VSO[1]	V/PSO[2]	OTA[3]	CPTA[4]
Virtual Data Centers	Create virtual data center	—	—	•	•
	Decommission virtual data center	—	—	•	•
	Modify VDC size	—	—	•	•
	Add network to VDC	—	—	•	•
	Remove network from VDC	—	—	•	•
Users and IAC Roles	Add or remove a user as a Server Owner	—	—	•	•
	Assign or remove a Cloud Provider Technical Administrator	—	—	—	•
	Assign or remove Organization Technical Administrator	—	—	•	•
	Modify user properties	—	—	•	•
	View Cloud Provider Technical Administrator role settings	—	—	—	•
	View Organization Technical Administrator role settings	—	—	•	•
	View Virtual Server Owner role settings	—	—	—	•
	View Virtual and Physical 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 physical server	•	•	•	•
	Power-up, power-down, power-cycle a Virtual Machine	•	•	•	•
	Take, revert-to, or remove a server snapshot	•	•	•	•
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	—	—	—	•

Table 1-1 Capabilities by User Role

Category	Service	VSO[1]	V/PSO[2]	OTA[3]	CPTA[4]
Organizations	Add or remove an Organization	—	—	—	•
	Add, modify, or remove an organization	—	—	—	•
	Create, modify, remove organization networks	—	—	—	•
	Add or modify the Cloud Administration organization	—	—	—	•

1. Virtual Server Owner
2. Virtual and Physical Server Owner
3. Organization Technical Administrator
4. Cloud Provider Technical Administrator

CHAPTER 2

Ordering Cloud Services

Cloud Portal hosts the customer-facing element of Cisco Intelligent Automation for Cloud 3.1 (IAC), where users log in and order services.

This chapter provides information and steps for commissioning and decommissioning servers. It includes the following sections:

Commissioning a Virtual Machine and Installing an Operating System

Deploy a virtual machine with your chosen operating system in the cloud system.

Step 1 Choose **My Workspace** from the module drop-down list and click the **Order Cloud Services** tab.

Figure 2-1 Order Cloud Services Portal

Step 2 On the Order Servers portal, click **Order a Virtual Machine and Install an OS**.

Note The asterisk * next to a field indicates that it is a required field and must contain a valid value.

Step 3 On the Order a Virtual Machine and Install an OS form, specify the following information.

Field	Action
VDC Name	Choose the VDC 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)
Guest Operating System Family	Choose **Windows** or **Linux**.
Operating System	Choose platform and version number of the operating system.

Field	Action
Operating System Template	Choose the template that you want to use to create the new virtual machine. (The selections in this drop-down depend on the operating system that you select.) Only Operating Systems Templates that are registered for the Cisco Server Provisioner as the VDC POD are shown. To register an operating system template, see Registering an Operating System Template, page 3-53.
Computer Name (Host)	Enter a unique name for the new virtual machine.
Virtual Machine Size	Choose a server size form the drop-down list. 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, select the option from the drop-down list. The values automatically populate the display-only fields immediately under the drop-down list.
Deploy to Network	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.
Lease Term	*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 5-3.
Enter password Re-enter password	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.

Step 4 Click **Submit Order**.

Commissioning a Virtual Machine from a Template

Deploy a virtual machine using a template with pre-configured settings.

Step 1 Choose **My Workspace** from the module drop-down and click the **Order Cloud Services** tab.

Step 2 On the Order Services portal (Figure 2-1 on page 2-2), click **Order a Virtual Machine From Template**.

Note The asterisk * next to a field indicates that it is a required field and must contain a valid value.

Step 3 On the Order a Virtual Machine From Template form, choose or enter the information shown in the following table.

Field	Action
VDC	Choose the VDC 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)
Operating system family	Choose **Windows** or **Linux**
Operating system	Choose platform and version number of the operating system
VM template	Choose the template that you want to use to create the new virtual machine. (The selections in this drop-down depend on the operating system that you select.) Only VM Templates that are registered and in the same data center as the VDC POD are shown. To register an VM template, see Registering a Virtual Machine Template, page 3-52.
Computer Name (Host)	Enter a name for the new virtual machine. The name must be unique.
Virtual Machine Size	Choose a server size form the drop-down list. 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, select the option from the drop-down list. The values automatically populate the display-only fields immediately under the drop-down list.
Deploy to Network	Choose a network whose static IP address will be assigned to the new virtual machine.

Term	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 5-3.
Enter password Re-enter password	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.

Step 4 Click **Submit Order**.

Decommissioning a Virtual Machine

Power-off and permanently remove an existing virtual machine from the Cloud resource pool, and release all associated resources for re-use.

Step 1 Choose **My Workspace** from the module drop-down and click the **My Servers** tab.

Step 2 On the My Servers portal (Figure 3-7 on page 3-12), locate and click the name of the virtual machine that you want to decommission.

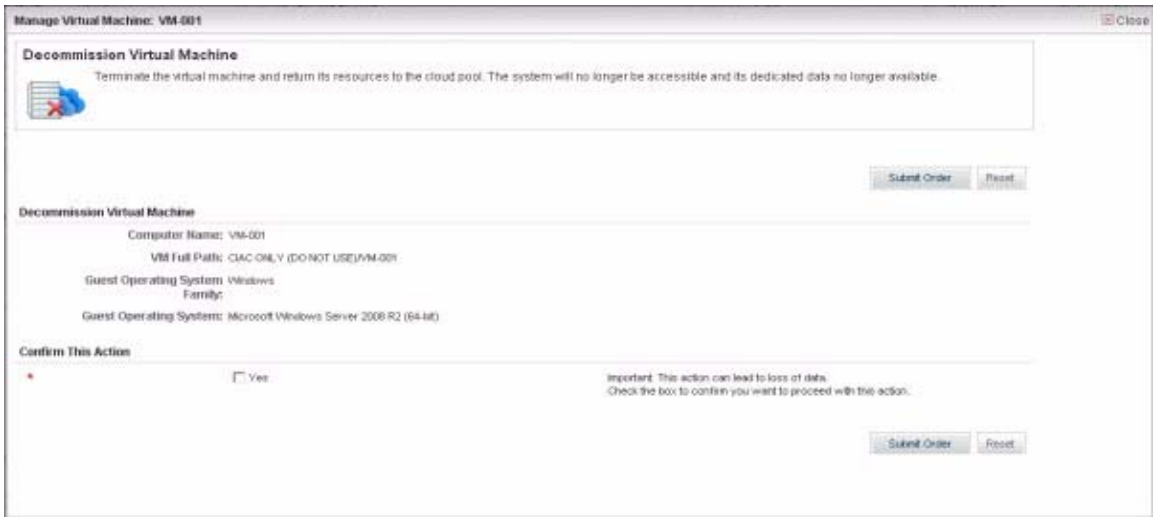
Detailed information about the virtual machine and icons for performing actions appear in the Take Action panel.

Step 3 Click the **Decommission** icon.

The Decommission Virtual Machine form displays the computer name, full path, and operating system.

Step 4 Click the **Yes** checkbox to confirm the decommission.

Figure 2-2 Decommission Virtual Machine Form



Step 5 Click **Submit Order**.

Commissioning a Physical Server

Note Virtual Server Owners do not have permissions to order physical servers.

Deploy a physical server with Windows or Linux operating system installed.

Step 1 Choose **My Workspace** from the module drop-down and click the **Order Cloud Services** tab.

Step 2 On the Order Cloud Services portal (Figure 2-1 on page 2-2), click **Order a Physical Server**.

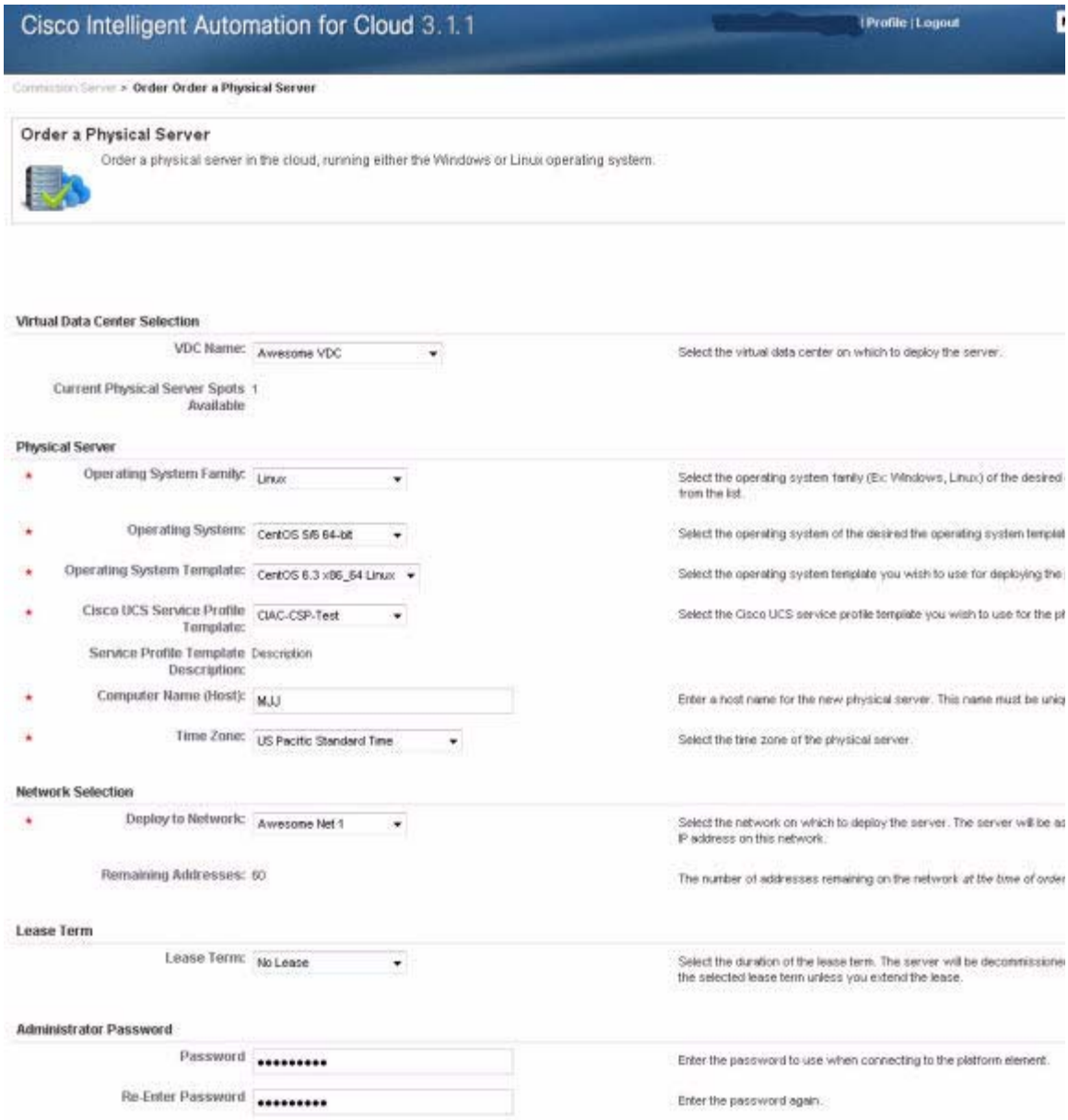
Note The asterisk * next to a field indicates that it is a required field and must contain a valid value.

Step 3 On the Order a Physical Server form, choose or enter the information shown in the following table.

Field	Action
VDC	Choose a VDC 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)
Operating system family	Choose **Windows** or **Linux**
Operating system	Choose platform and version number of the operating system
Operating System Template	Choose the template that you want to use to create the new physical server. (The selections in this drop-down depend on the operating system that you select.) To register an operating system template, see Registering an Operating System Template, page 3-53. Only Operating System Templates that are registered for the Cisco Server Provisioner as the VDC POD are shown.
Cisco UCS Service Profile Template	Choose the UCS server profile template that you want to use to create the new physical server. (The selections in this drop-down depend on the operating system that you select.) To register a UCS service profile template, see Modifying Email Notification Templates, page 3-55.
Computer Name (Host)	Enter a name for the new server. The name must be unique. I
Computer time zone	Choose the time zone of the physical location of the new server.
Deploy to Network	Choose a network whose static IP address will be assigned to the new virtual machine.

Term	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, Storage Expiration Date. For more information server lease terms and expiration dates, see Managing Server Leases, page 5-3.
Enter password Re-enter password	Enter and 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.

Figure 2-3 Order a Physical Server Form



Step 4 Click **Submit Order**.

Decommissioning a Physical Server

Power down and permanently remove an existing physical server, including power off, from the Cloud resource pool, and release all associated resources for re-use.

Step 1 Choose **My Workspace** from the module drop-down and click the **My Servers** tab.

Step 2 On the My Servers portal (Figure 3-7 on page 3-12), locate and click the name of the physical server that you want to decommission.

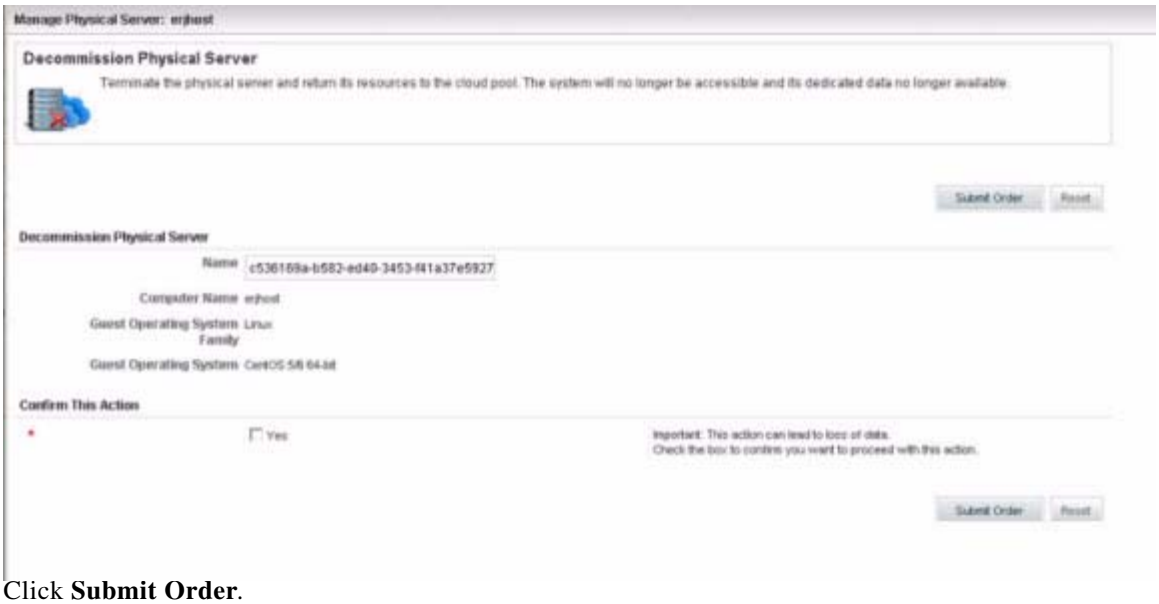
Detailed information about the server and icons for performing actions appear in the Take Action panel.

Step 3 Click the **Decommission** icon.

The Decommission Physical Server form displays the computer name, time zone, and operating system.

Step 4 Check the **Yes** radio button to confirm the decommission.

Figure 2-4 Decommission Physical Server Form



Step 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. 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.

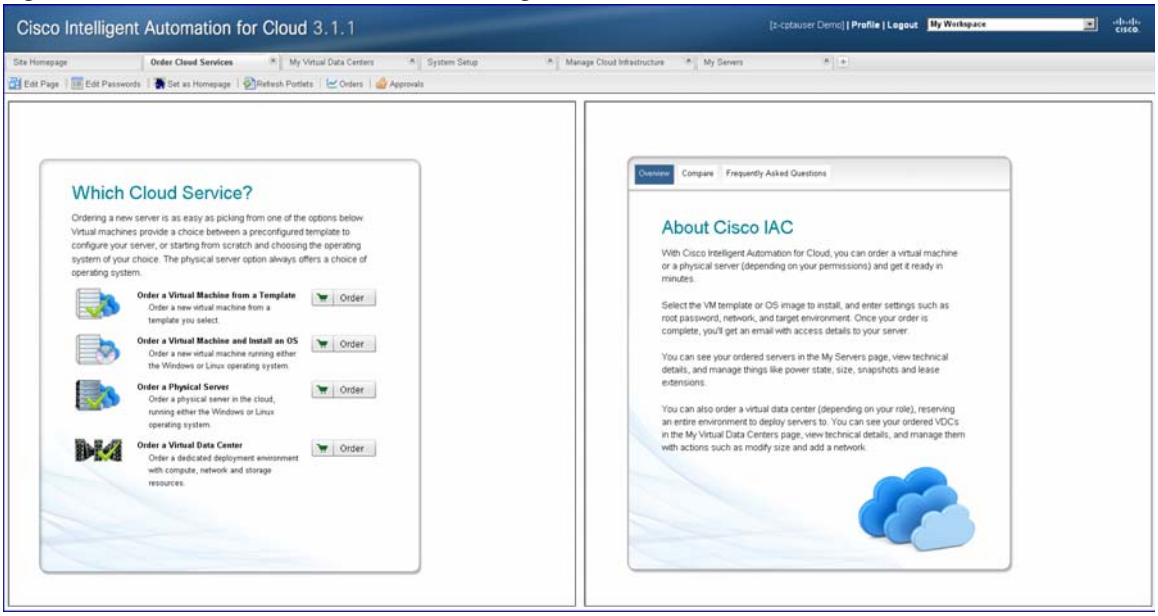
You must be either an Organization Technical Administrator or Cloud Provider Technical Administrator to create a virtual data center. Create Virtual Data Center ordered by an Organization Technical Administrator requires authorization by the Cloud Provider Technical Administrator.

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.

Tip You may only define one virtual data center in Cisco IAC SE.

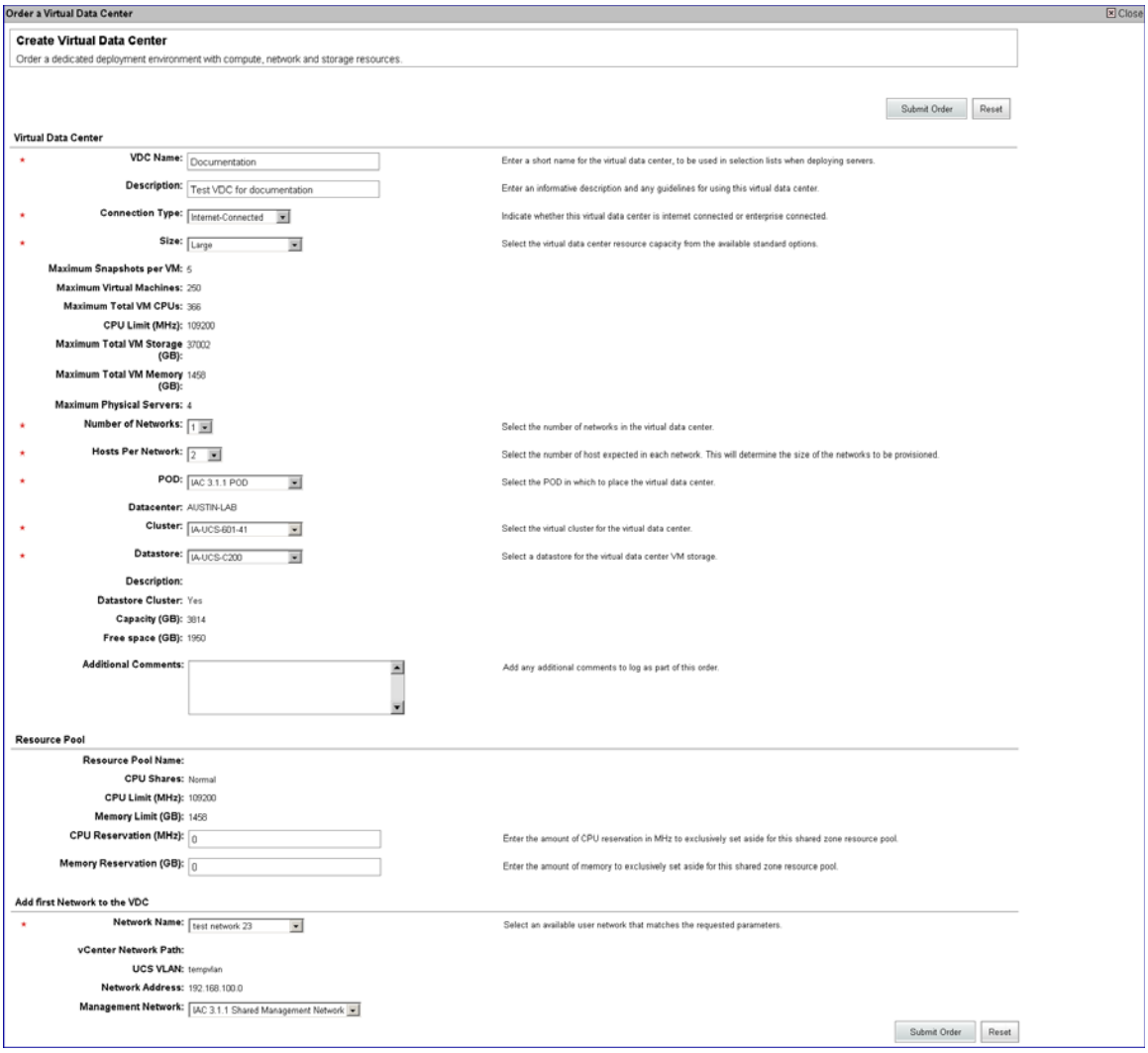
Step 1 Choose **My Workspace** from the module drop-down list and click the **Order Cloud Services** tab.

Figure 2-5 Virtual Data Center Portal Page



Step 2 Under Which Cloud Service, click **Order a Virtual Data Center** to create a new virtual data center.

Figure 2-6 Create Virtual Data Center form



Step 3 On the Create Virtual Data Center form, 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 select the virtual data center.
Description	Enter a description for the virtual data center.
Connection Type	Indicates whether this shared zone is connected to the internal network. Select Internet-Connected or Enterprise-Connected.
Size	Select the size of the virtual data center. The size determines the maximum limits for the number of virtual servers, maximum number
Maximum Snapshots per VM	Read-only field determined by the VDC size selected. This limits the maximum number of snapshots allowed per virtual server.

Field	Action
Maximum Virtual Machines	Read-only field determined by the VDC size selected. This limits the maximum number of virtual server allowed in the virtual data center.
Maximum Total VM CPUs	Read-only field determined by the VDC size selected. This limits the maximum number of vCPUs allowed in the virtual data center. The number of vCPUs is determined based on the server size for the virtual server.
CPU Limit (MHz)	Read-only field determined by the VDC size selected. A VMware resource pool is created with CPU limit size (MHz) limit defined for the VDC size.
Maximum Total VM Storage (GB)	Read-only field determined by the VDC size selected. This limits the maximum amount of storage utilization allowed in the virtual data center. The amount of storage used is determined based on the server size for the virtual server.
Maximum Total VM Memory (GB)	Read-only field determined by the VDC size selected. This limits the maximum amount of storage utilization allowed in the virtual data center. The amount of storage used is determined based on the server size for the virtual server.
Maximum Physical Servers	Read-only field determined by the VDC size selected. This limits the maximum number of physical servers allowed in the virtual data center.
Number of Networks	A virtual data center can contain multiple networks. Select the number of networks for this virtual data center. If more than one network is selected, additional **Add Network** sections will be displayed on the form.
Hosts per network	Select 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.
Additional Comments	Provide any additional information that is needed for the cloud provider technical administrator to create the virtual data center.

Step 4 Click **Submit Order**. The requisition will go to the Cloud Provider Technical Administrator for approval.

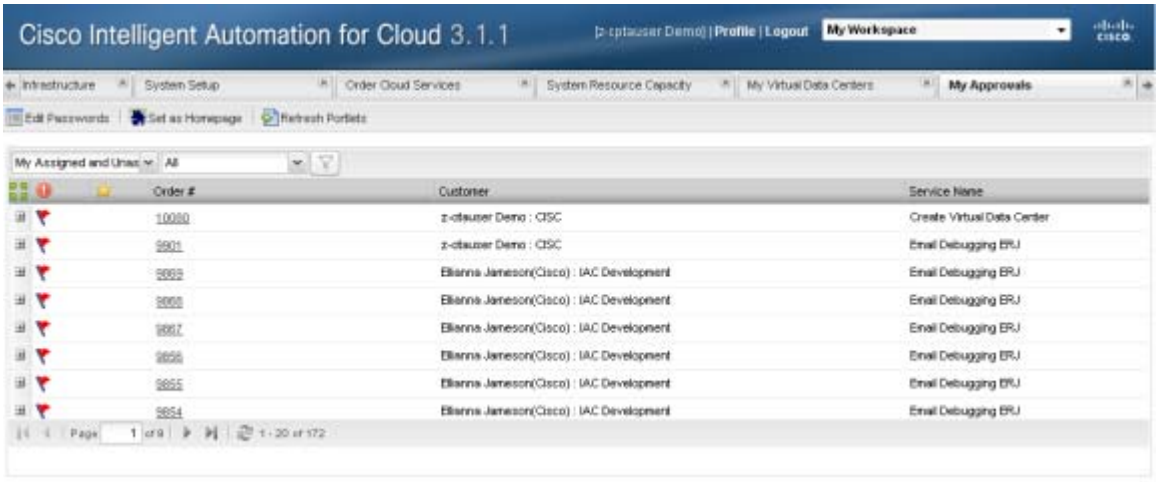
Approvals for Create Virtual Data Center

Note You must be a Cloud Provider Technical Administrator or an Organization Technical Administrator to perform this action.

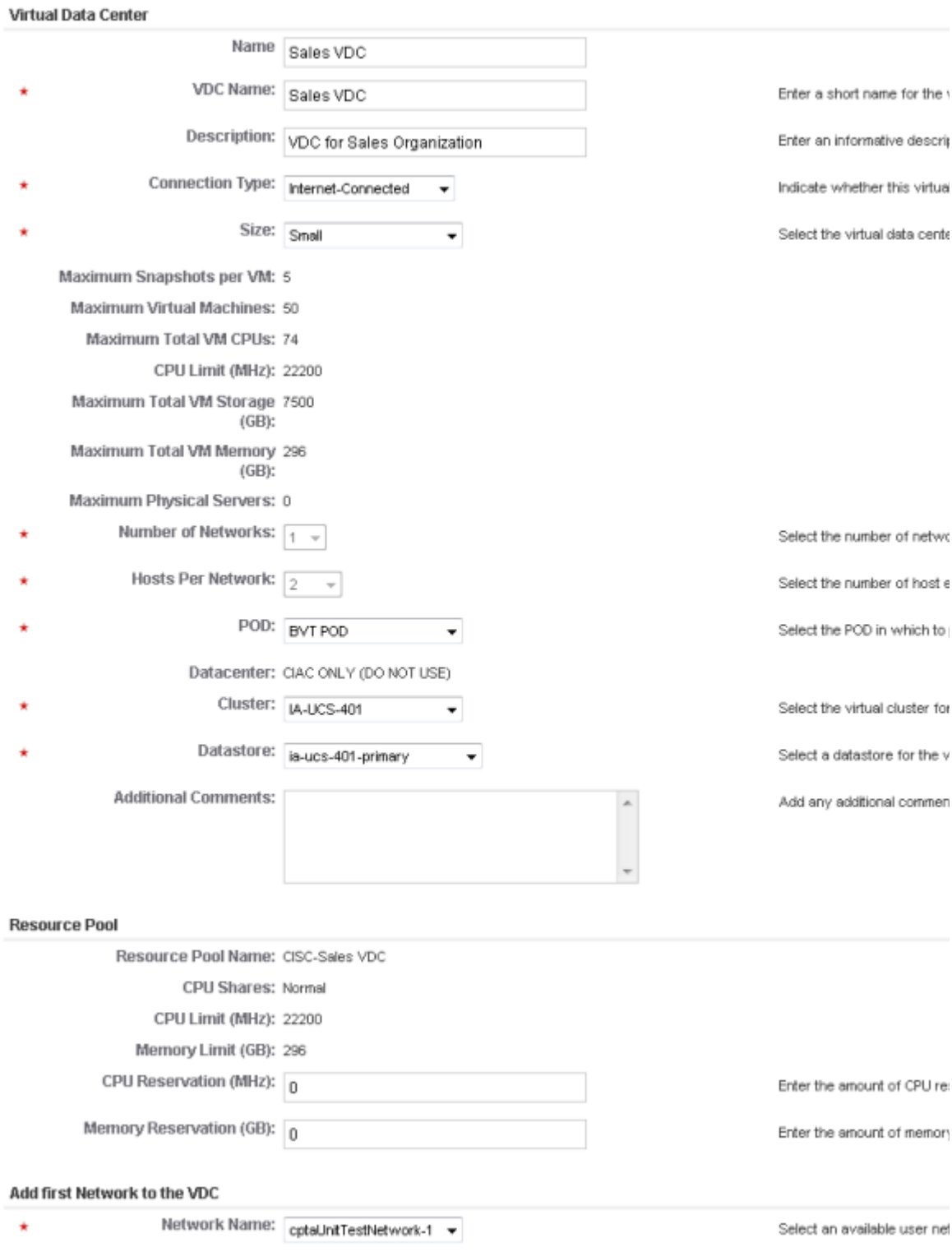
When an Organization Technical Administrator submits a requisition for Order a Virtual Data Center, it goes the CPTA's Cloud Service Approval Administrator queue for approval. The Cloud Provider Technical Administrator must assign a POD, cluster, datastore, and networks for the virtual data center, as part of the approval process.

Step 1 Choose **My Workspace** from the module drop-down list and click **My Approvals** tab

Figure 2-7 Create Approval



Step 2 Click on **Order #** to create a virtual data center requisition that requires approval. This brings up the requisition form.



Step 3 Select the POD that this virtual data center should be created on. The POD selection should be based on the virtual data center size selected and available capacity in the POD.

Step 4 Select the cluster that this virtual data center should be created on. The cluster selection should be based on the virtual data center size selected and available capacity in the cluster. A single cluster can host multiple virtual data centers.

Step 5 Select the datastore that this virtual data center will use. The datastore selection should be based on the virtual data center size selected and available capacity of the datastore. A single datastore can be associated with multiple virtual data centers.

Step 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 selected. This corresponds directly to the VMware resource pool CPU reservation.

Step 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 selected. This corresponds directly to the VMware resource pool memory reservation.

Step 8 Select 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 selection should be based on the Hosts per Network specified in the requisition.

Step 9 Optionally, a management network can be associated with a virtual data center. If desired, select a management network for the virtual data center. The management network subnet size should be the same as the user network size.

Step 10 If the virtual data center has more than one network, repeat steps 8-9 for each network.

Step 11 Click **Update** to update the requisition with the VDC resource assignment information.

Step 12 Click **Approve**.

Decommissioning a Virtual Data Center

Note You must be an Organization Technical Administrator or a Cloud Provider Technical Administrator to perform this action.

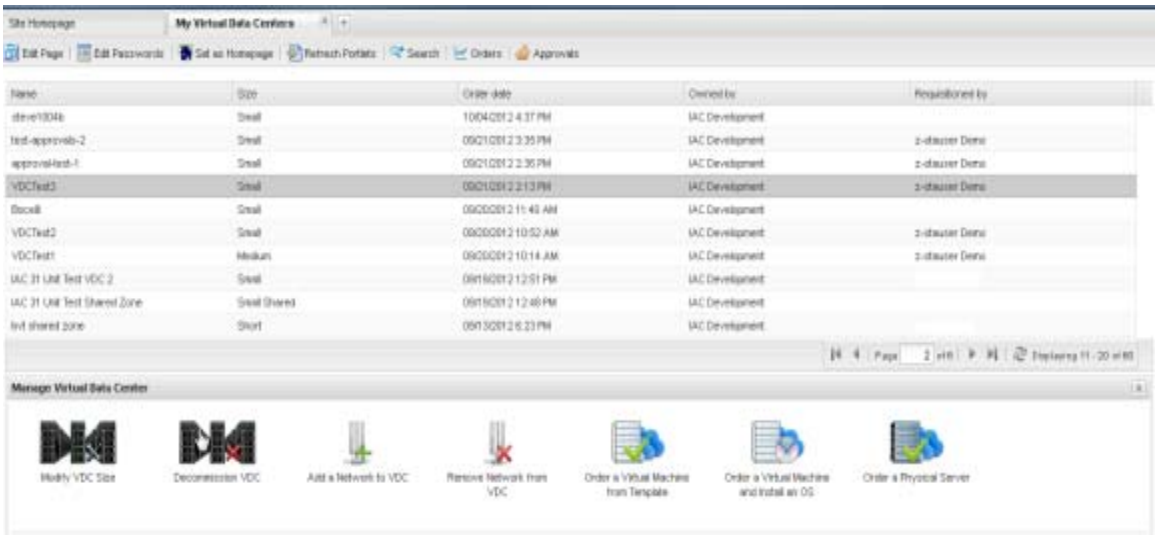
Note All networks, virtual machines and physical machines must be removed from the virtual data center prior to decommissioning.

Step 1 In Cloud Portal, choose **My Workspace** from the module drop-down list, then click **My Virtual Data Centers**.

Step 2 Locate the virtual data center in the grid, then click the name.

Step 3 In the Manage Virtual Data Center collapsible panel, click on **Decommission VDC**.

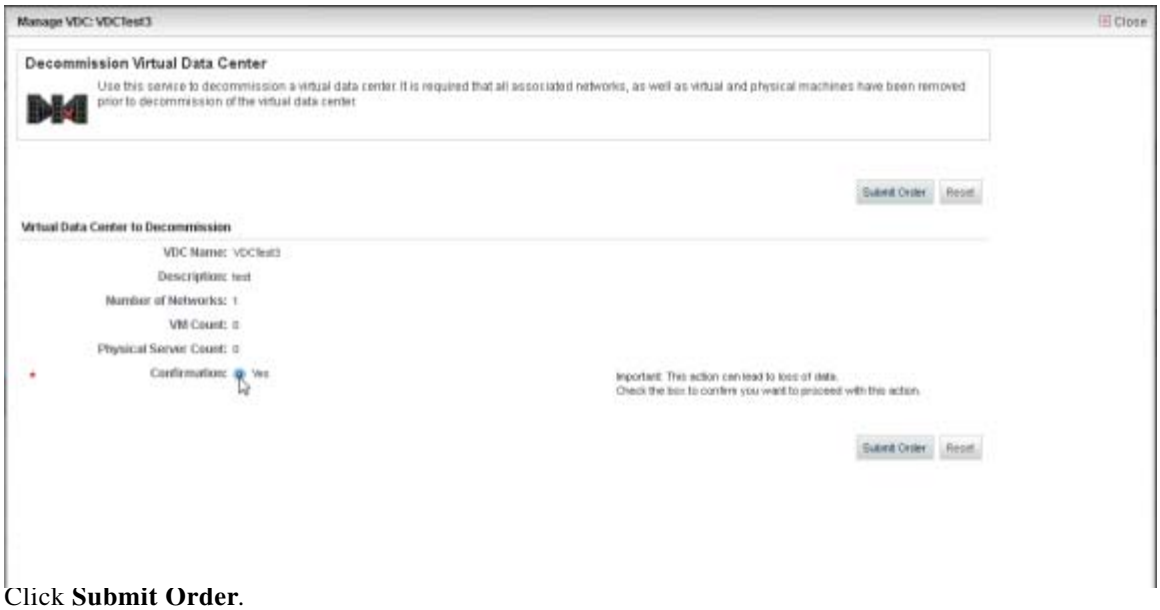
Figure 2-8 Decommission Virtual Data Center



Note NOTE: In the modal window that follows the VDC Name field will be prepopulated with the selected virtual data center name.

Step 4 Click the radio button to confirm action.

Figure 2-9 Decommission VDC Form



Step 5 Click **Submit Order**.

CHAPTER 3

Managing the Cloud System

Note To perform many of the procedures covered in this guide, you must have access to portals in the form of tabs in My Workspace. To add portals to My Workspace, see Adding Portal Page Access to My Workspace, page 1-5.

After the initial set up of your cloud system, there are tasks you must perform the keep the system running smoothly.

This chapter provides information on managing the resources in your cloud system. It includes the following sections:

Managing Resources

This section describes how to use the My Servers, System Resources, and CloudSync services to view specifications and status, and discover new virtual and physical servers, blades, blade chassis, and data centers. It includes the following subsections:

Viewing System Resource Capacity

On the System Resources portal you can 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
- Statuses of physical blades in the pool
- Number of unoccupied slots in the physical blade chassis

Note You must be a Cloud Provider Technical Administrator to perform this action.

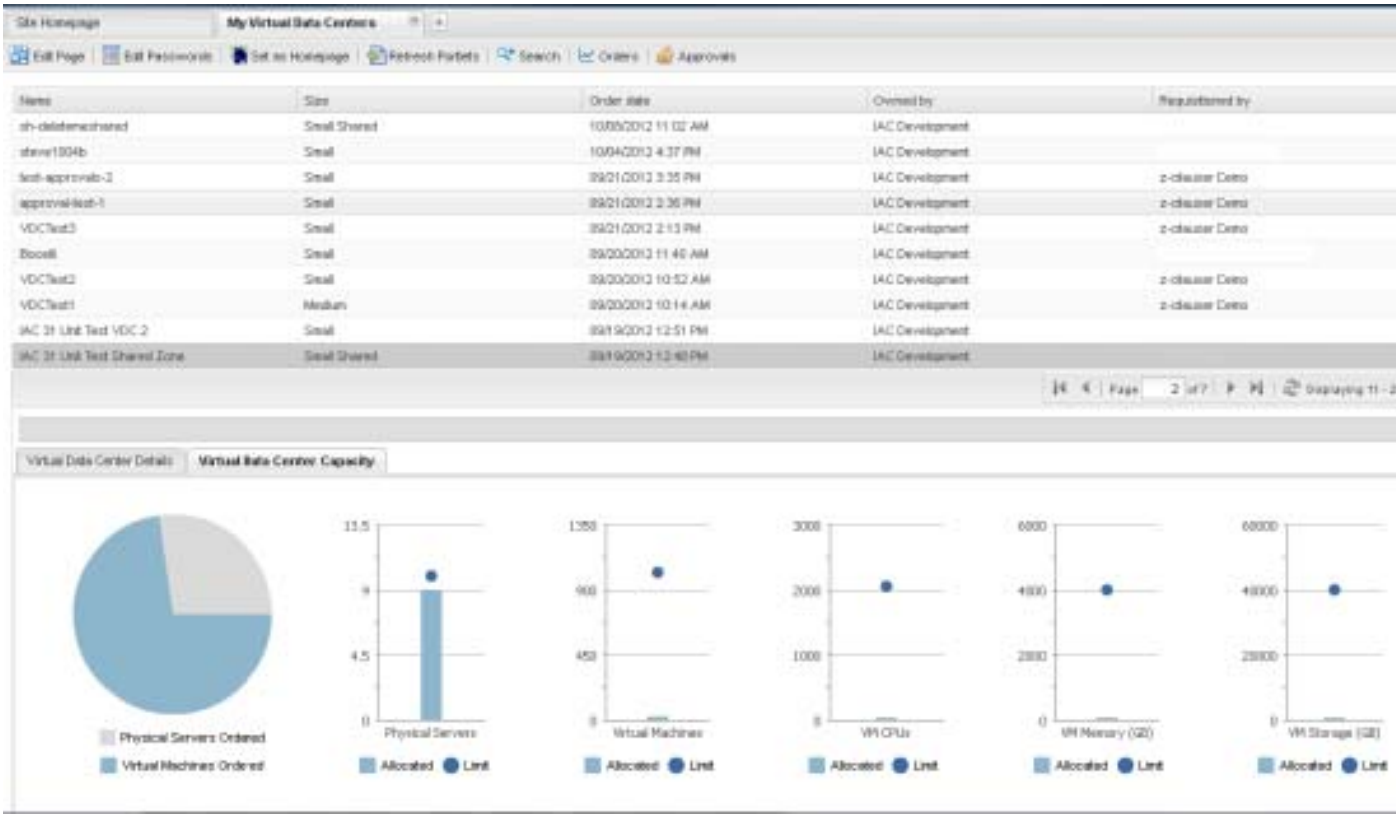
Step 1 Choose **My Workspace** from the module drop-down list and then click the **System Resources** tab.

The System Resources portal (Figure 3-1 on page 3-3) displays following information

Resource	Description
Virtual Cluster Capacity	Indicates CPU and memory resource capacity and allocation for each vCenter cluster. • 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.
UCS Blade Pool Management	Pie chart showing the proportions of Cisco UCS blades in the physical, virtual, and management pools.

UCS Blade Pool Management Physical	Pie chart showing the proportions of physical blades in the management pool that are in of the following states: • Available—The blade is not commissioned or in use by end-users and is available to be commissioned. • In Use—The blade is commissioned and in use by end-users. • Pending—The blade is in transition between blade pools. **Note** For information on Cisco UCS blades and blade pools, see Managing Blade Pools, page 3-37.
Physical Blade Chassis Occupancy	Identifies the number of unoccupied slots in the Cisco UCS chassis.

Figure 3-1 System Resources Portal Page



Managing Cloud Infrastructure Discovery

This section describes the CloudSync Infrastructure Discovery service, which detects changes to objects in the cloud infrastructure.

- Overview, page 3-4
- Discovering Objects in the Cloud Infrastructure, page 3-5

- Viewing Discovered Objects in the Infrastructure, page 3-5

Overview

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 the following types of objects:

- VMware vCenter Datacenter—Clusters, hosts, datastores, Resource pools, portgroups, and VM templates
- Cisco Server Provisioner—Operating system templates
- Cisco UCS Manager—Service profile templates, UCS blades, and UCS VLANs

After discovery, objects are placed into a Discovered state, where some are auto-registered (data centers, clusters, hosts, resource pools, port groups, and UCS VLANs), and others wait to be managed into service or rejected. In this transitional state, 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.

You can 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 reregistered using the Activate action.

Figure 3-2 shows the Discovery portal, located on the Manage Cloud Infrastructure tab in the My Workspace 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.

Figure 3-2 CloudSync Infrastructure Discovery Portal

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, Cisco Server Provisioner, or Cisco UCS Manager.
- Discover all new and existing instances of all objects.

Note You must be a Cloud Provider Technical Administrator to perform this action.

Step 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**.

Step 2 Click the Discover link to open the Discover Infrastructure form.

Step 3 Click **Submit Order**.

To discover all instances of a platform element type:

Step 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**.

Step 2 Click the Discover link to open the Discover Infrastructure form.

Step 3 Click **Submit Order**.

To discover all new instances of all objects:

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

Step 2 Click **Submit Order**.

Viewing Discovered Objects in the Infrastructure

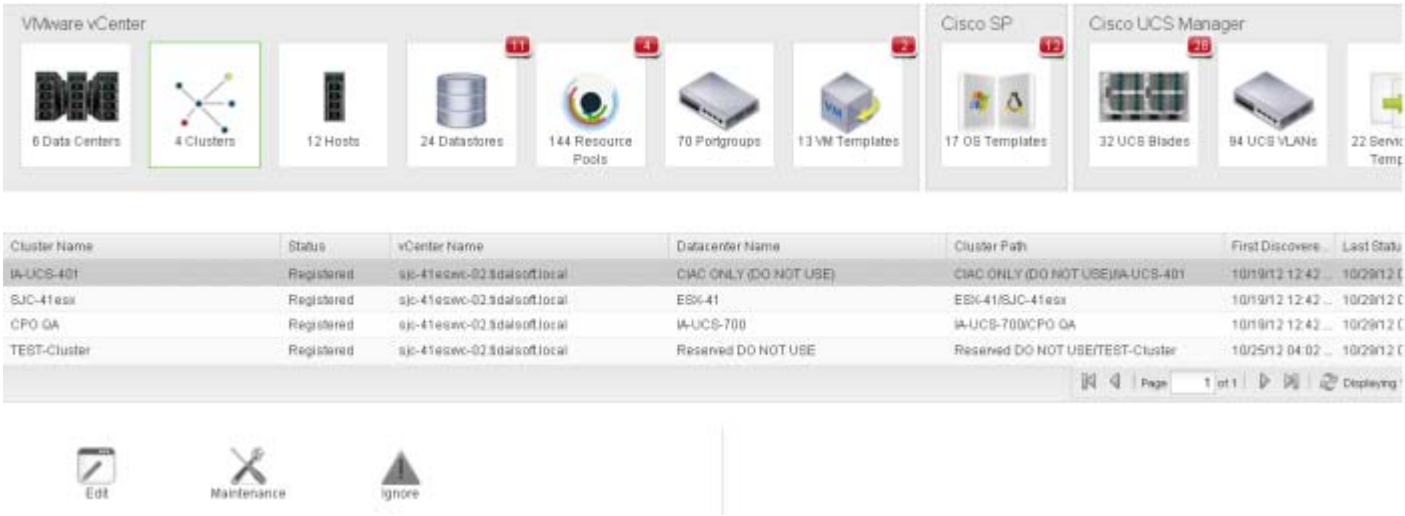
View instances of all objects that were added to the system or detected during the last discovery (if any).

To view all instances of an object, click the icon of the object—for example, **Clusters**.

As shown in Figure 3-3, 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.

Note To customize the columns that display in the grid, see Customizing Table Views, page 1-15.

Figure 3-3 CloudSync Infrastructure Discovery—vCenter Clusters



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.

As shown in Figure 3-3, 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.

With the exception of Not Found, you can transition the status of an object to another status. (See Table 3-1 on page 3-7.)

Figure 3-4 State Transitions

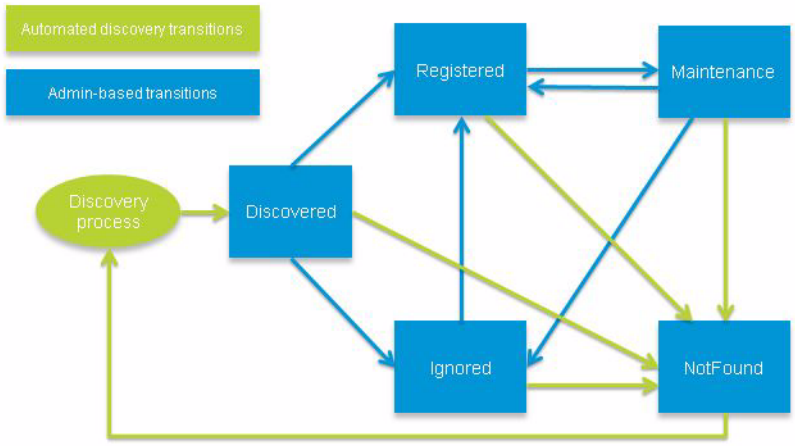


Table 3-1 Allowed Discovered State Transitions

	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

Validating Platform Configuration

If you need to troubleshoot infrastructure or connection settings, you can test the configurations for the platform elements (VMware vCenter, Cisco UCS Manager, Cisco Server Provisioner), Cisco Process Orchestrator, email server, and share (dropbox) location.

The following sections provide instructions for performing validations:

- Validating the Platform Elements
- Validating Cisco Process Orchestrator and Share Location Settings, page 3-10
- Validating the Email Server Connection, page 3-10

Validating the Platform Elements

On the Connection Status portal, the Platform Elements frame displays icons for all three platform element types. If there are multiple instances of UCS Manager, Cisco Server Provisioner, or both, the number of instances appears below the icon.

For the platform elements, you have two options:

- Validating an Individual Platform Element
- Validating All of the Platform Elements Together

Validating an Individual Platform Element

Perform the following procedure to validate any of the platform element types individually.

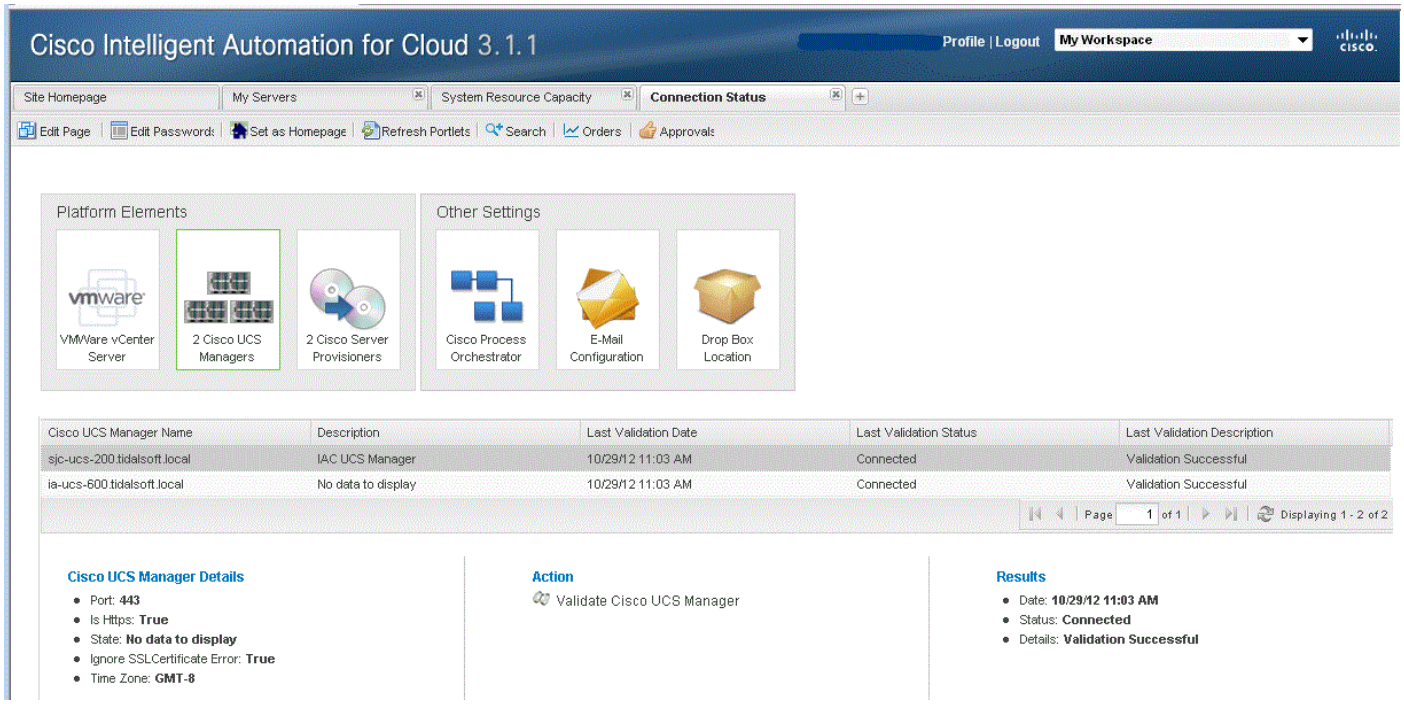
Step 1 In My Workspace, click the **Connection Status** tab to open the Connection Status portal.

Figure 3-5 Connection Status Portal

Step 2 Click the icon for the platform element that you want to validate.

The Take Action grid and details about the platform appear. The grid displays results of the last validation (if any).

Figure 3-6 Validate the Cisco UCS Manager Platform Element



Step 3 Click the platform element listing in the grid, then click the icon beside **Validate** to open the Validate Platform Element form.

Step 4 If multiple instances of the platform element exist, choose the one that you want to validate from the Name drop-down list.

Step 5 Click **Submit Order** to send the order and display the order confirmation form.

Step 6 Close the order confirmation form.

After the order is submitted, the system performs the validation.

Step 7 Repeat Step 2 through Step 6 for other platform elements as needed.

Step 8 To view the results when the validation process is complete, return to the Connection Status portal and click the icon for the platform element. The results display in the grid with the proper time stamp. If the results do not appear, wait ten minutes, then return or refresh the screen.

Validating All of the Platform Elements Together

Perform the following procedure to validate all of the platform elements—VMware vCenter Server, Cisco UCS Manager, and Cisco Server Provisioner—together.

Note To view the results when the validation process is complete, return to the Connection Status portal and click the icon for the platform element. The results display in the grid with the proper time stamp. If the results do not appear, wait ten minutes, then return or refresh the screen.

Step 1 In My Workspace, click the **Connection Status** tab to open the portal.

Step 2 Click inside the Platform Elements frame.

Step 3 Click the icon beside **Validate All Platform Elements** to open the form.

Step 4 On the Validate Platform Element form, click **Submit Order** to send the order and display the order confirmation form.

Step 5 Close the order confirmation form.

After the order is submitted, the system performs the validations.

Step 6 To view the results when the validation is complete, return to the Validate Platform Configuration portal and click the icon for the platform element. The results display in the grid with the proper time stamp. If the results do not appear, wait ten minutes, then return or refresh the screen.

Validating Cisco Process Orchestrator and Share Location Settings

Perform the following procedure to test Cisco Process Orchestrator or share location.

Step 1 On the Connection Status portal, click the **Cisco Process Orchestrator** icon.

The Take Action grid and details about Process Orchestrator appear.

Step 2 Click the icon beside **Validate Cisco Process Orchestrator** to open the form.

Step 3 Click the **Cisco Process Orchestrator** listing in the grid, then click the icon beside **Validate Cisco Process Orchestrator** to open the form.

Step 4 Click **Submit Order** to send the order and display the order confirmation form.

After the order is submitted, the system performs the validation.

Step 5 Repeat Step 1 through Step 4 for Share Location.

Step 6 To view the results when the validations are complete, return to or refresh the Connection Status portal and click the icon for the object.

Step 7 The results display in the grid with the proper time stamp. If the results do not appear, wait ten minutes, then return or refresh the screen.

Validating the Email Server Connection

Perform the following steps to validate the email server connection.

Step 1 On the Connection Status portal, click the **Email Configuration** icon.

The Take Action grid and details about email server appear. The grid displays results of the last validation (if any).

Step 2 Click the email server listing in the grid, then click the icon beside **Validate Email Configuration** to open the form.

Step 3 Enter your valid email address in the Recipient Email Address field, then click **Submit Order** to send the order and close the form.

If the email server connection is valid, you will receive a system email confirming the validation.

Note If you do not receive the validation confirmation email, check the configuration of the SMTP server.

Managing Virtual Machines

This section describes management tasks on deployed virtual machines. It includes the following subsections:

Viewing Server Status and Properties

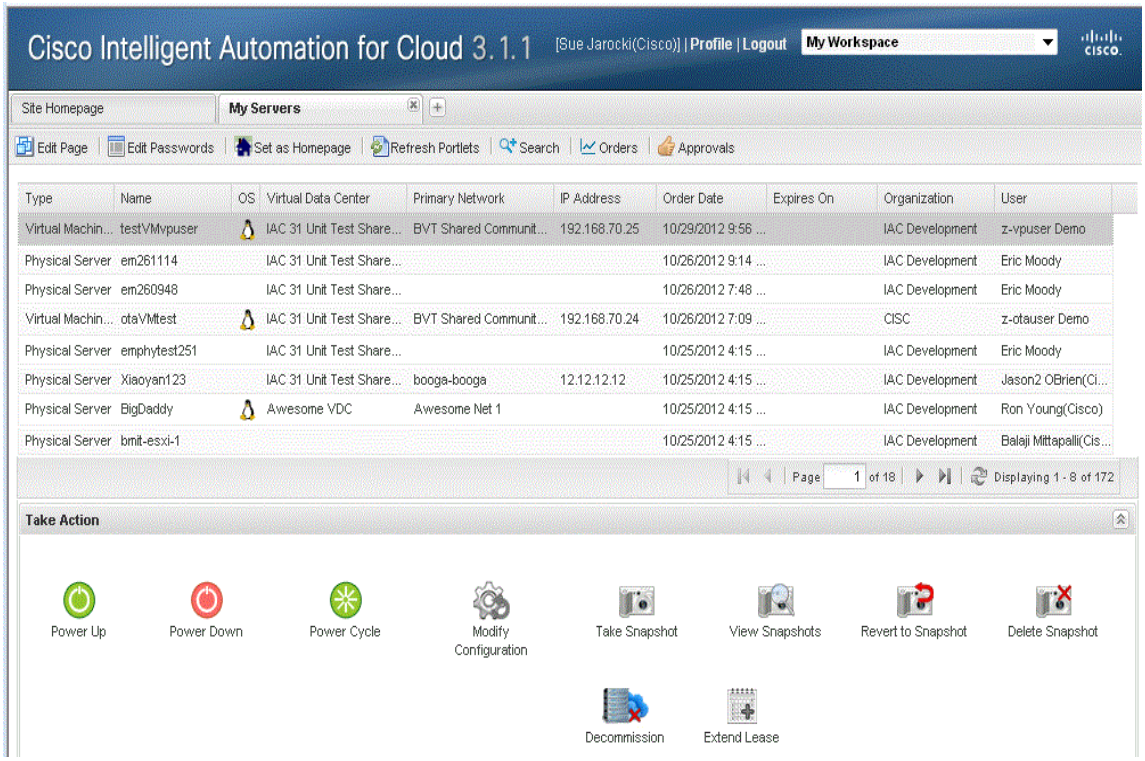
The My Servers portal provides information about all of your active servers. You can monitor status, manage snapshots, verify that a server you that ordered has been delivered, and manage power, modify configuration, take snapshots, decommission, and extend an existing lease.

Step 1 Choose **My Workspace** from the module drop-down list and the **My Servers** tab.

The My Servers portal (Figure 3-7 on page 3-12) displays active servers in a table with information about each server, including type (virtual or physical), operating system, organization, and Server Owner.

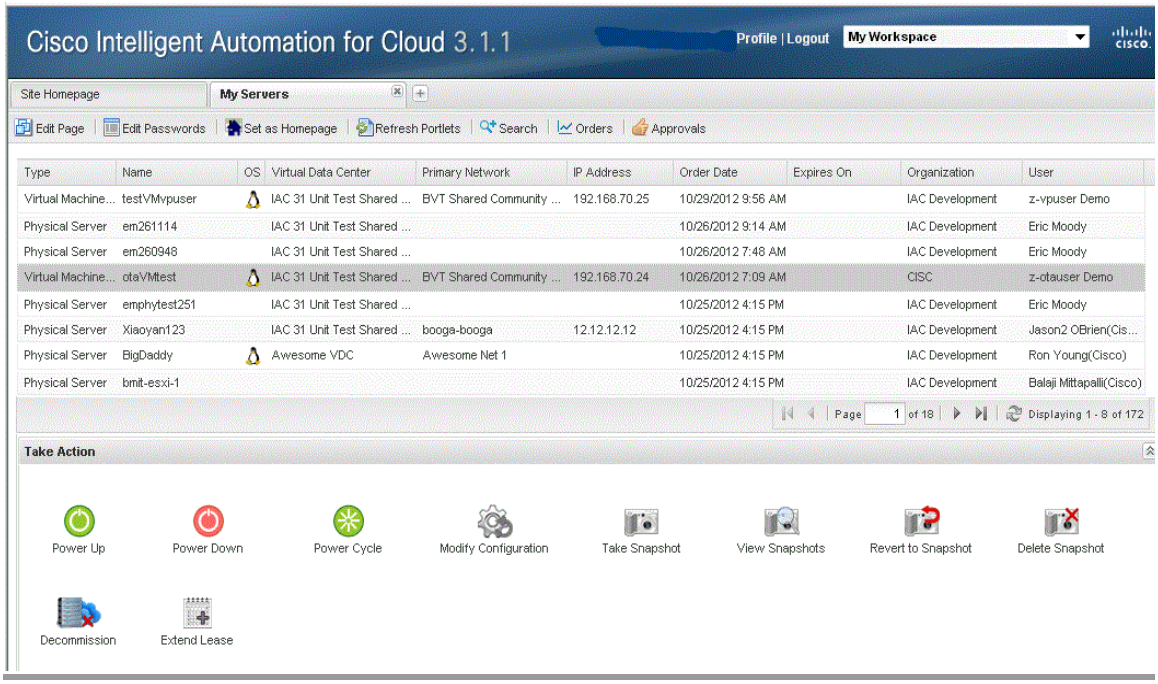
Note Additional columns are available. To add columns to the table, and to re-sort the rows, see Customizing Table Views, page 1-15.

Figure 3-7 My Servers Portal Page



Step 2 To display more details about a server or take action (see list of actions below), click the server name in the My Servers table to display the Take Action panel.

Figure 3-8 My Servers Portal Page Showing Take Action Panel



To take action on a server, click its name, then click one of the following icons in the Take Action pane:

- Power Down—See Powering Down a Virtual Machine, page 3-15
- Power Cycle—See Power-cycling a Virtual Machine, page 3-16
- Power Up—See Powering Up a Virtual Machine, page 3-16
- Decommission—See Decommissioning a Virtual Machine, page 2-6 or Commissioning a Physical Server, page 2-7
- Extend Lease—See Extending or Removing a Server Lease, page 5-4
- Modify Configuration—*Virtual machines only.* See Changing the Server Size of a Virtual Machine, page 3-13
- Take Snapshot, Revert to Snapshot, or Delete Snapshot—(Virtual machines only) See Managing Snapshots of Virtual Machines, page 3-18

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

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 and Installing an Operating System, page 2-2 and Commissioning a Virtual Machine from a Template, page 2-4.

Note The vCPU and vRAM values are set for each server size option and cannot be changed individually.

Step 1 Choose **My Workspace** from the module drop-down list and then click the **My Servers** tab.

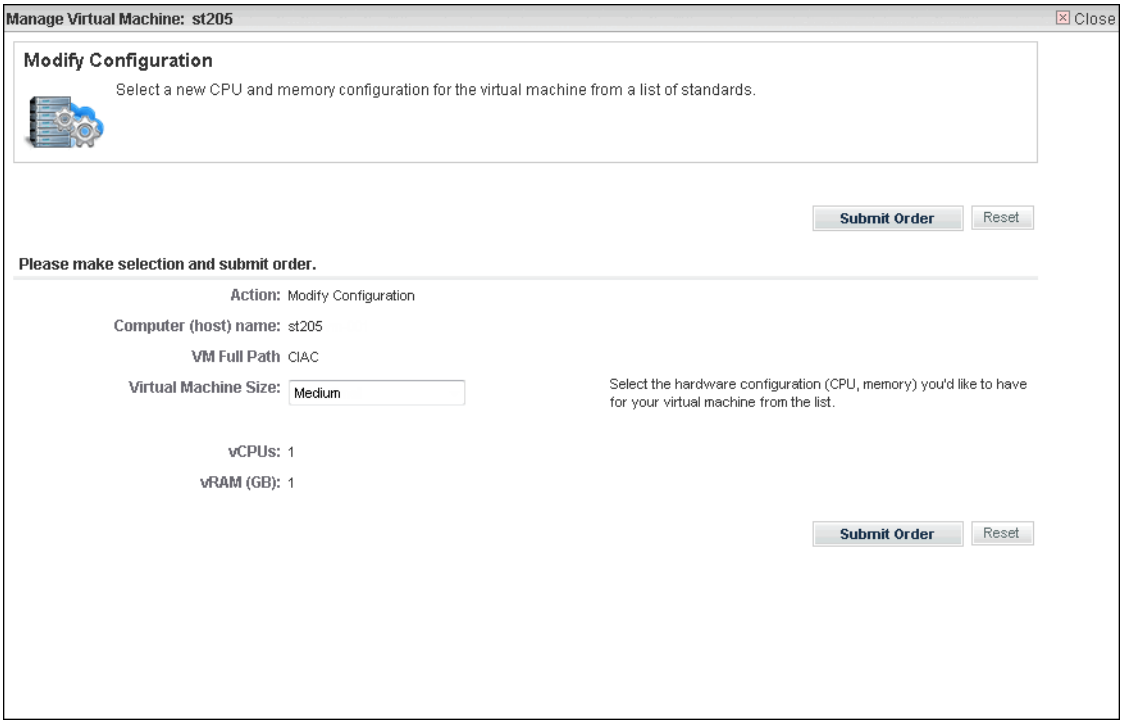
Step 2 On the My Servers portal (Figure 3-7 on page 3-13), locate and click the server in the My Servers panel.

Step 3 In the Take Action panel, click the **Modify Configuration** icon.

Step 4 On the Modify Configuration form, choose a size from the **Virtual Machine Size** drop-down list.

Note Available server size options are customizable by Administrators, and so may vary from the default options that ship with Cisco IAC 3.1. 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.

Figure 3-9 Virtual Machine—Modify Configuration



Step 5 Click **Submit Order**.

Managing Power on a Virtual Machine

Powering Down a Virtual Machine

Power down an active virtual machine, regardless of its operating system state.

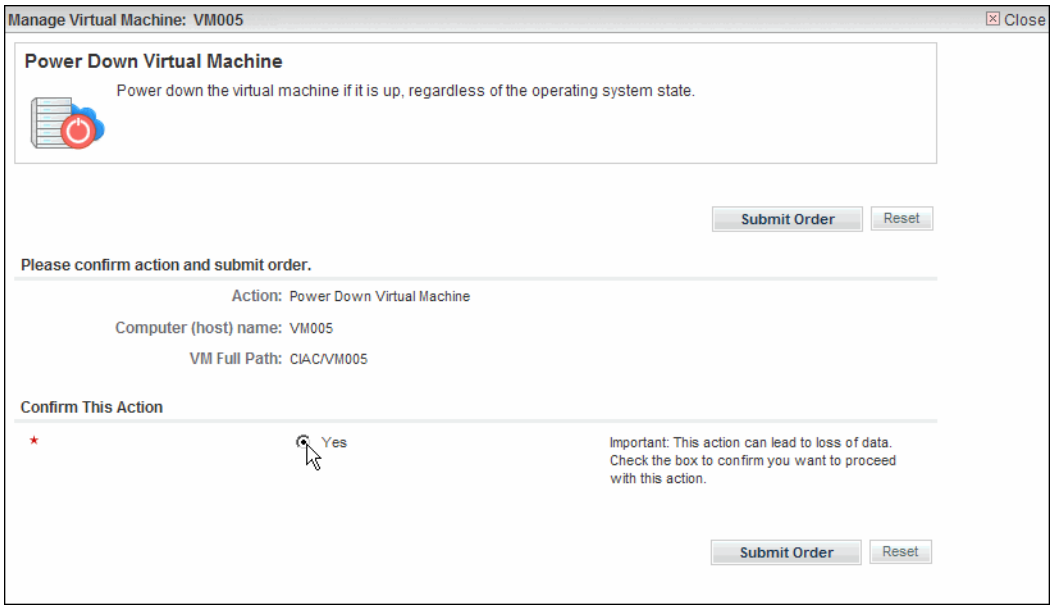
Note To remove a server from use, see Decommissioning a Virtual Machine, page 2-6.

Step 1 Choose **My Workspace** from the module drop-down list and then click the **My Servers** tab.

Step 2 On the My Servers portal page (Figure 3-7 on page 3-12), click the name of the virtual machine to display the Take Action panel (Figure 3-8 on page 3-13).

Step 3 Click the **Power Down** icon to open the Power Down Virtual Machine form.

Figure 3-10 Power Down Virtual Machine Form



Step 4 In the Confirm Action area, click the Confirm This Action radio button if you are sure the selected server is the one that you want to power down.

Step 5 Click **Submit Order**.

Power-cycling a Virtual Machine

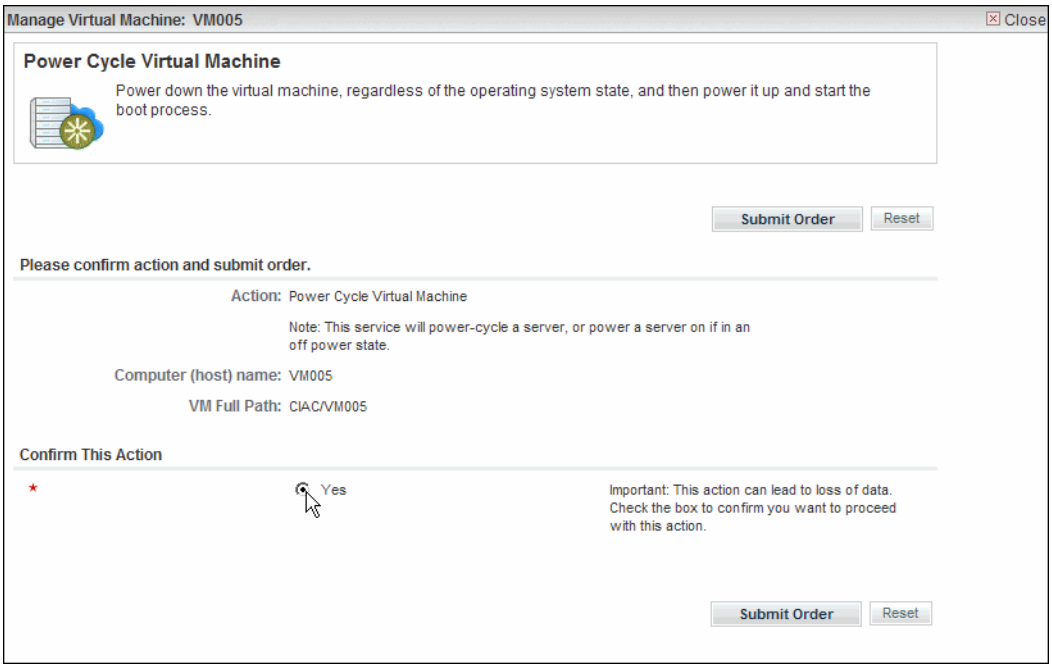
Use the power-cycle service to power-down a virtual machine, regardless of its operating system state, then power it up and start the boot process.

Step 1 Choose **My Workspace** from the module drop-down list and then click the **My Servers** tab.

Step 2 On the My Servers portal page (Figure 3-7 on page 3-12), click the name of the virtual machine to display the Take Action panel (Figure 3-8 on page 3-13).

Step 3 Click the **Power Cycle** icon to open the Power Cycle Virtual Machine form.

Figure 3-11 Power Cycle Virtual Machine Form



Note The asterisk * next to a field indicates that it is a required field and must contain a valid value.

Step 4 In the Confirm Action area, check the check box if you are sure the selected server is the one that you want to power cycle.

Step 5 Click **Submit Order**.

Powering Up a Virtual Machine

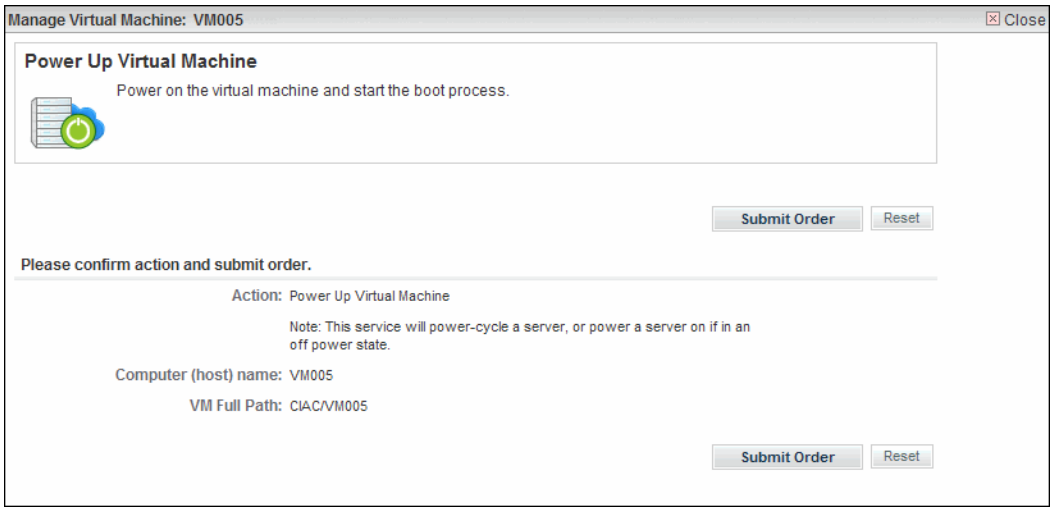
Power up a virtual machine that has been powered-down, and start the boot process.

Step 1 Choose **My Workspace** from the module drop-down list and then click the **My Servers** tab.

Step 2 On the My Servers portal page (Figure 3-7 on page 3-12), click the name of the virtual machine to display the Take Action panel (Figure 3-8 on page 3-13).

Step 3 Click the **Power Up** icon to open the Power Up Virtual Machine form.

Figure 3-12 Power Up Virtual Machine Form



Step 4 If you are sure the selected server is the one that you want to power up, click **Submit Order**.

Managing Snapshots of Virtual Machines

Create, revert to, view an archive of, and remove snapshots of virtual machines.

Taking a Snapshot of a Virtual Machine

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

Step 1 Choose **My Workspace** from the module drop-down list and then click the **My Servers** tab.

Step 2 On the My Servers portal page (Figure 3-7 on page 3-12), click the name of the virtual machine to display the Take Action panel (Figure 3-8 on page 3-13).

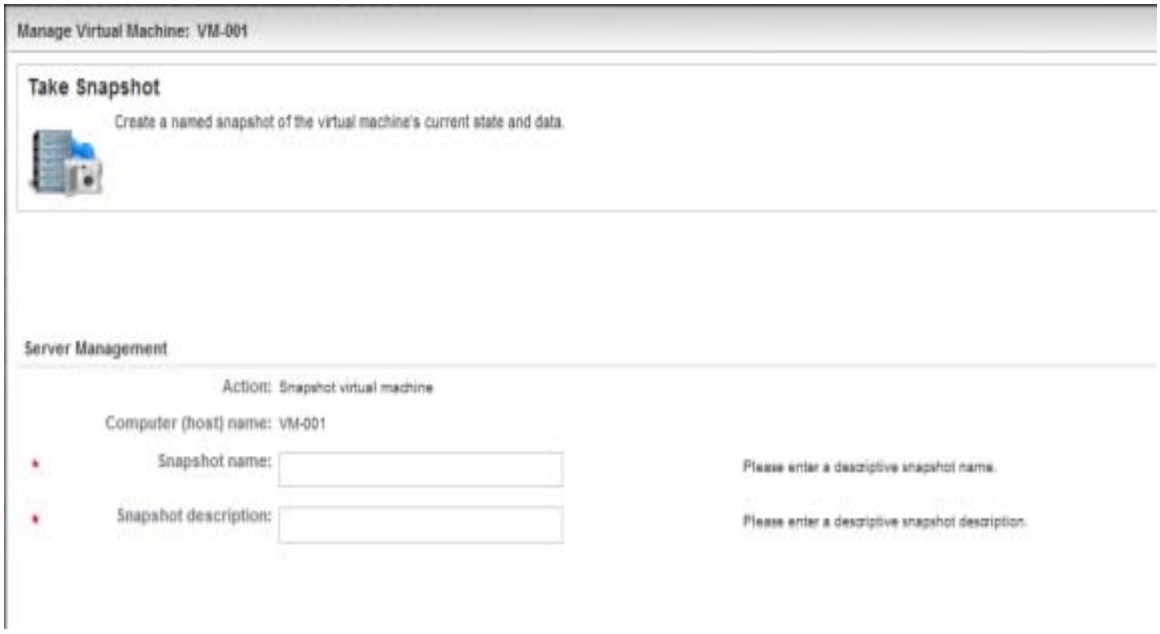
Step 3 Click the **Take Snapshot** icon to open the Take Snapshot form.

Note The asterisk * next to a field indicates that it is a required field and must contain a valid value.

Step 4 In the snapshot name field, enter a unique and descriptive name for the snapshot.

Step 5 Enter a description of the snapshot.

Figure 3-13 Take Snapshot Form



Step 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.

Step 1 Choose **My Workspace** from the module drop-down list and then click the **My Servers** tab.

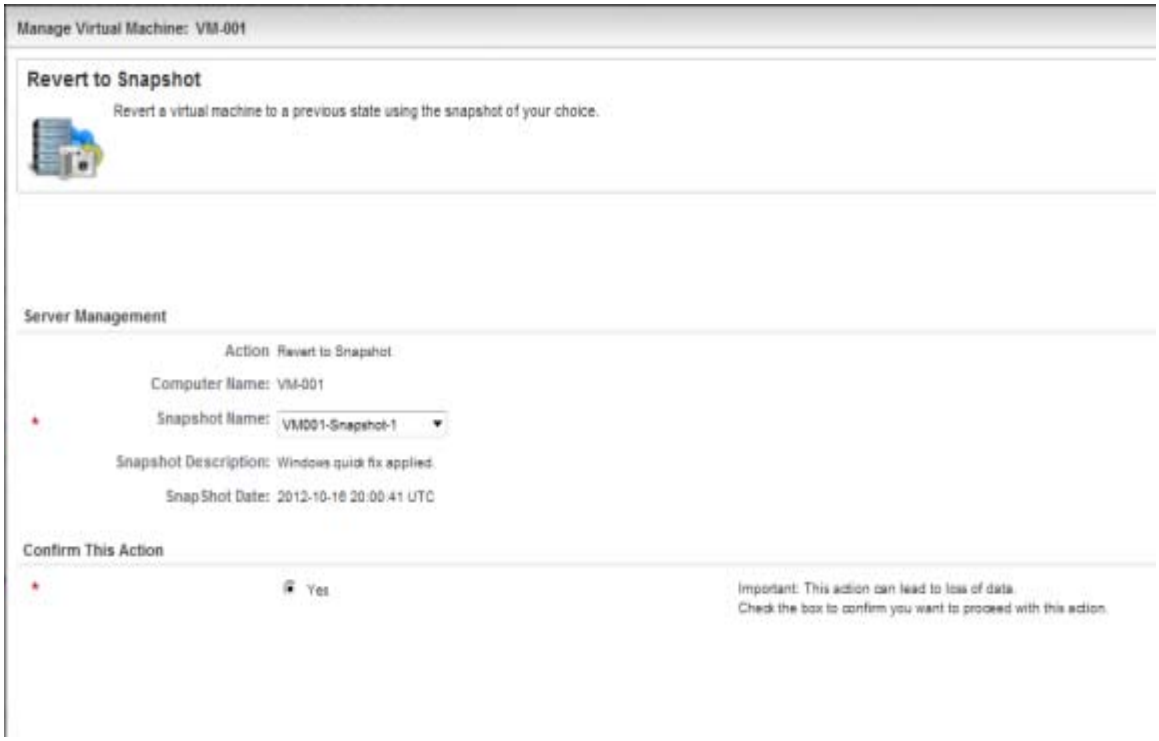
Step 2 On the My Servers portal page (Figure 3-7 on page 3-12), click the name of the virtual machine to display the Take Action panel (Figure 3-8 on page 3-13).

Step 3 Click the **Revert Snapshot** icon to open the Revert to Snapshot form.

Note The asterisk * next to a field indicates that it is a required field and must contain a valid value.

Step 4 From the Snapshot name drop-down list, choose the snapshot to which you want to revert the selected virtual machine.

Figure 3-14 Revert to Snapshot Form



Step 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

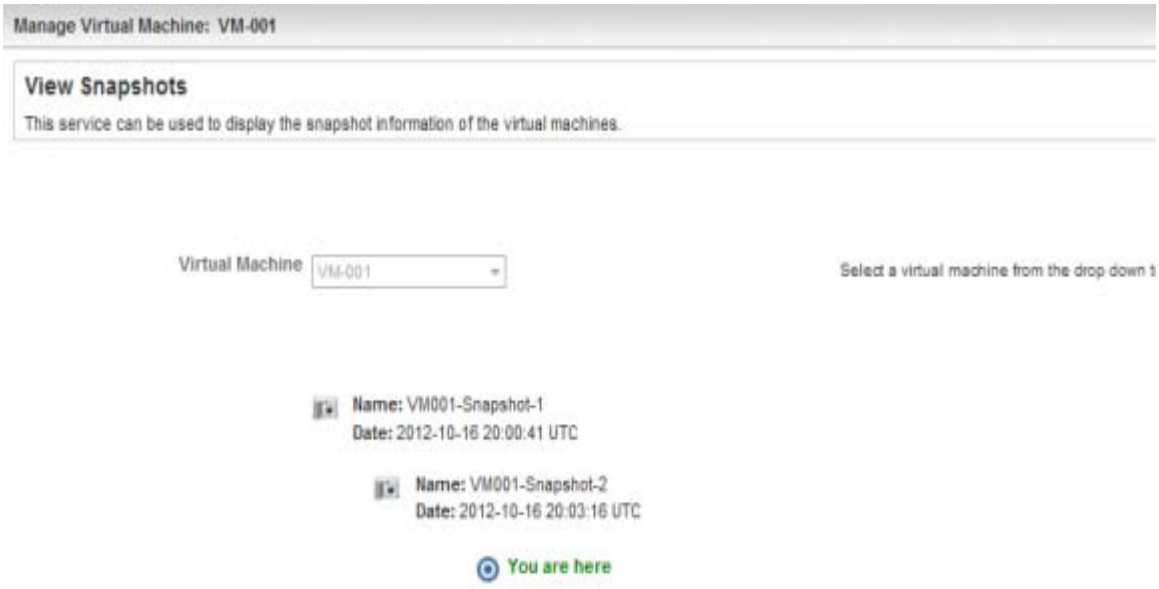
View the history of snapshots taken of virtual machines within an organization. From the list, you can view history and related services of a snapshot.

Step 1 Choose **My Workspace** from the module drop-down list and then click the **My Servers** tab.

Step 2 On the My Servers portal page (Figure 3-7 on page 3-12), click the name of the virtual machine to display the Take Action panel (Figure 3-8 on page 3-13).

Step 3 Click the **View Snapshots** icon to open the View Snapshot form

Figure 3-15 View Snapshot Form



Deleting a Snapshot

Permanently delete a virtual machine snapshot.

Step 1 Choose **My Workspace** from the module drop-down list and then click the **My Servers** tab.

Step 2 On the My Servers portal page (Figure 3-7 on page 3-12), click the name of the virtual machine to display the Take Action panel (Figure 3-8 on page 3-13).

Step 3 Click the **Delete Snapshot** icon to open the Delete Snapshot form.

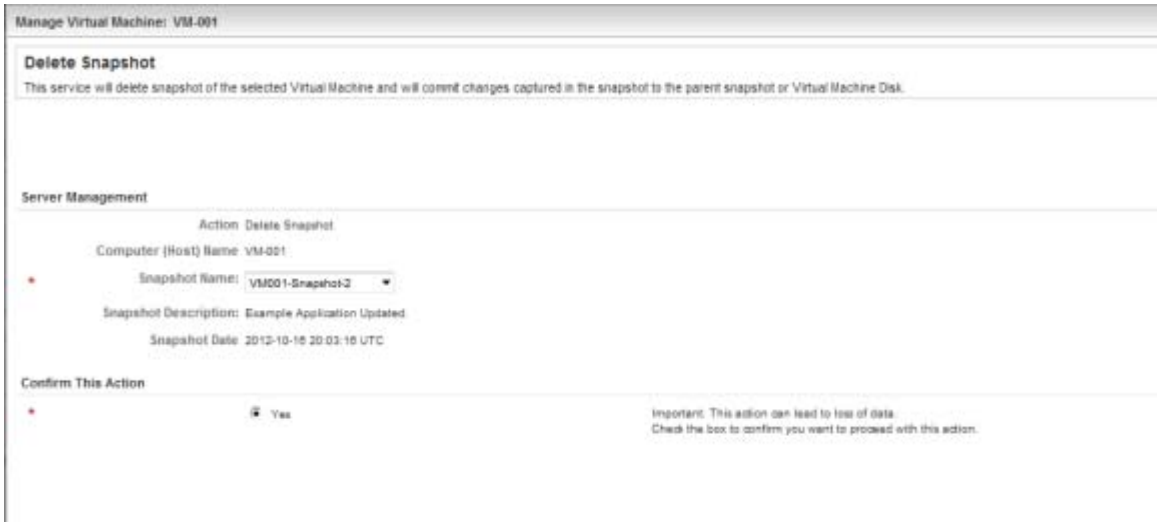
Note The asterisk * next to a field indicates that it is a required field and must contain a valid value.

Step 4 From the Snapshot name drop-down list, choose the snapshot to which you want to revert the selected virtual machine.

Step 5 Click **Submit Order**

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

Figure 3-16 Delete Snapshot Form



Step 6 Click **Submit Order**.

Managing Virtual Data Centers

Note Organization Technical Administrator or Cloud Provider Technical Administrator role is required for all Virtual Data Center actions.

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.

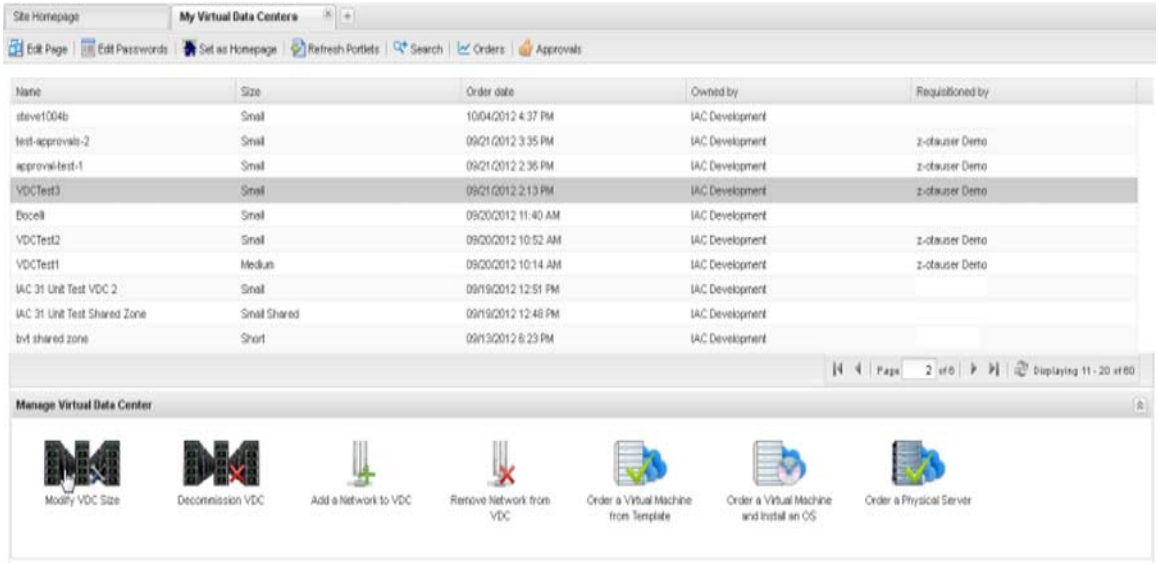
To change the resource pool size of a deployed virtual data center, complete the following steps:

Step 1 In Cloud Portal, choose **My Workspace** from the module drop-down list, then click **My Virtual Data Centers**.

Step 2 Locate the Virtual Date Center in the grid, then click the name.

Step 3 In the Manage Virtual Data Center collapsible panel, click on **Modify VDC Size**.

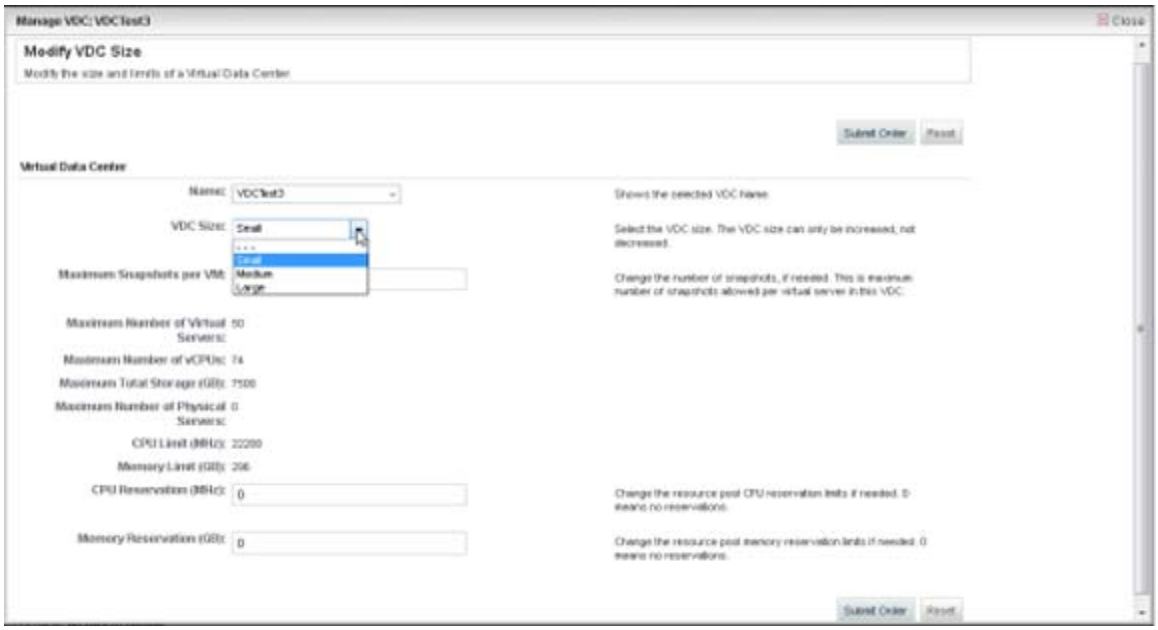
Figure 3-17 Modify Virtual Data Center Size



Note In the modal window that follows the Name field will be prepopulated with the selected virtual data center name. The current size and size settings populate the remaining fields.

Step 4 Choose a new size from the VDC Size drop-down list.

Figure 3-18 Manage VDC Form



Step 5 If needed, change the Maximum Snapshots per VM, CPU Reservation (MHz), Memory Reservation (GB).

Step 6 Click **Submit Order**.

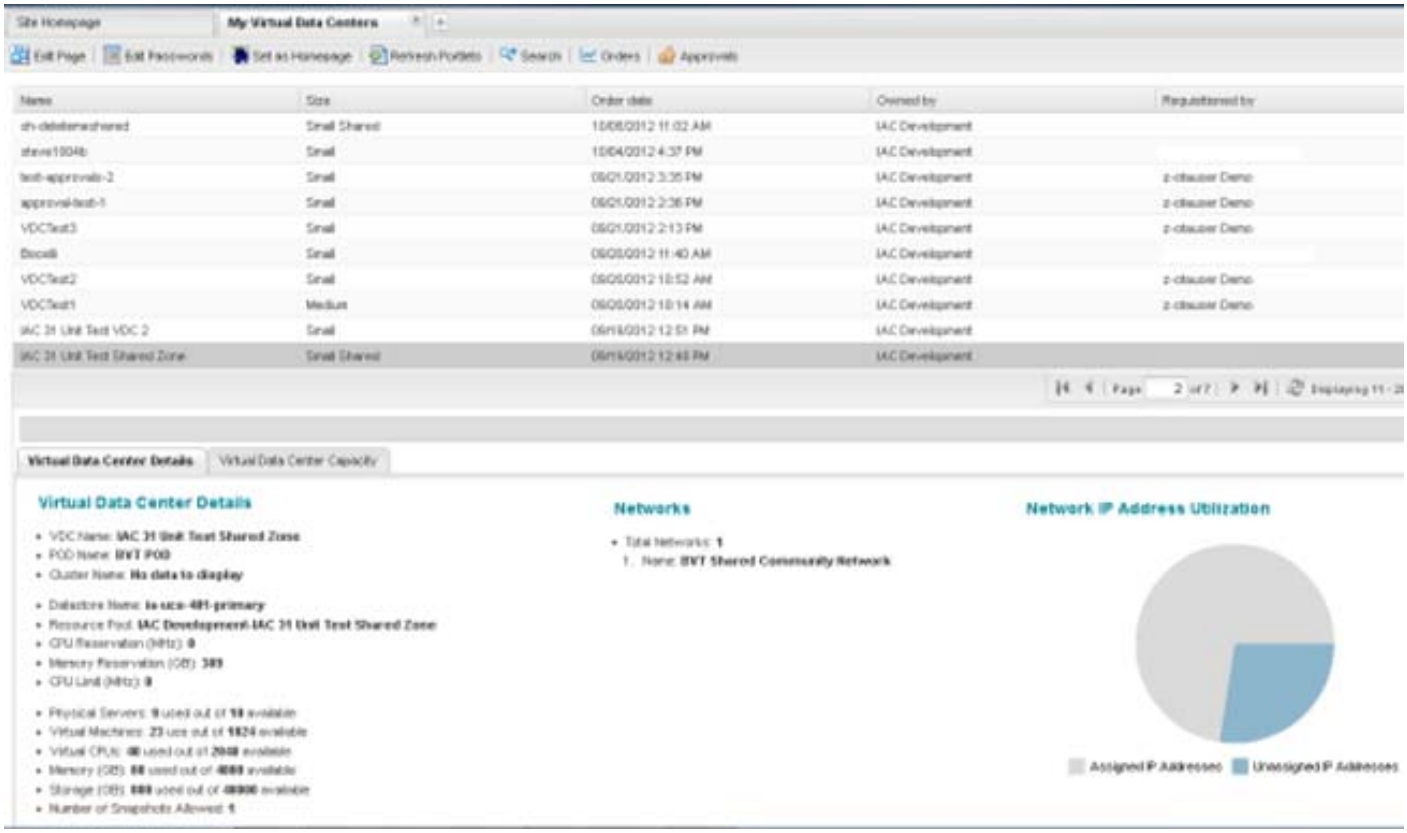
Viewing Virtual Data Center Details

To view in-depth details for a certain virtual data center:

Step 1 In Cloud Portal, choose **My Workspace** from the module drop-down list, then click **My Virtual Data Centers**.

Step 2 Locate the Virtual Date Center in the grid, then click the name.

Figure 3-19 Virtual Data Center Details



There is a tab panel at the bottom of the page. When you select 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 selected virtual data center:
  - Name of the virtual data center
  - The POD associated to the selected virtual data center
  - The Cluster associated to the selected virtual data center (NOTE: Only visible to the Cloud Provider Technical Administrator)
  - The Datastore associated to the selected virtual data center (NOTE: Only visible to the Cloud Provider Technical Administrator)
  - The Resource Pool associated to the selected 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 (NOTE: 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 (NOTE: Only visible to the Cloud Provider Technical Administrator)
  - The CPU limit (MHz) associated to the selected virtual data center
  - The total number of allocated Physical Servers versus the total number of available Physical Servers within the selected virtual data center.
  - The total number of allocated Virtual Machines versus the total number of available Virtual Machines within the selected virtual data center.
  - The total number of allocated Virtual CPUs (MHz) versus the total number of available Virtual CPUs (MHz) within the selected virtual data center.
  - The total number of allocated Memory (GB) versus the total number of available Memory (GB) within the selected virtual data center.
  - The total number of allocated Storage (GB) versus the total number of available Storage (GB) within the selected virtual data center.
  - The maximum number of snapshots allowed within the selected virtual data center.

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

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

Note If the values of both assigned and unassigned are zero no pie chart will be displayed. In its place will be No data to display.

Viewing Virtual Data Center Capacity Charts

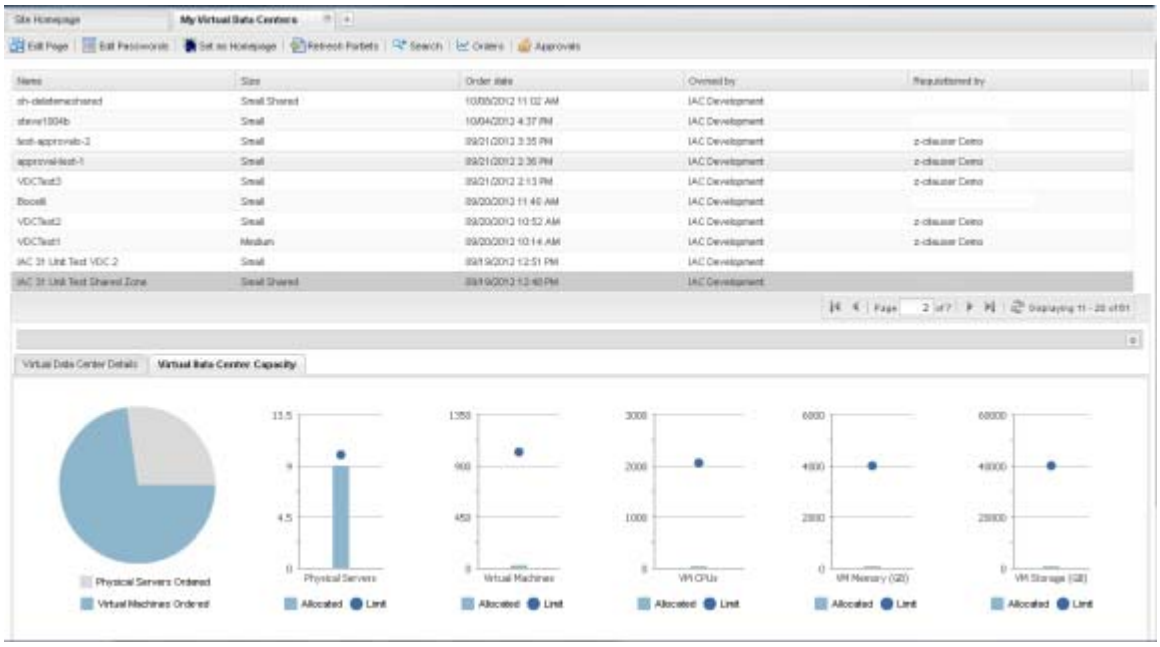
Note Cloud Provider Technical Administrator role is required for this action.

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

Step 1 In Cloud Portal, choose **My Workspace** from the module drop-down list, then click on **My Virtual Data Centers**.

Step 2 Locate the Virtual Date Center in the grid, then click the name.

Figure 3-20 Virtual Data Center Capacity Charts



Step 3 In the tab panel located at the bottom of the page, click the **Virtual Data Center Capacity** tab.

The following charts will populate:

- A pie chart showing the total number of virtual machines ordered versus the total number of physical servers ordered within the selected virtual data center.
- A bar chart showing the total number of physical servers allocated with a circular point indicating the limit (maximum number of) allowed within the virtual data center.
- A bar chart showing the total number of virtual machines allocated with a circular point indicating the limit (maximum number of) allowed within the virtual data center.
- A bar chart showing the total number of virtual machine CPUs (MHz) allocated with a circular point indicating the limit allowed within the virtual data center.
- A bar chart showing the total number of virtual machine Memory (GB) allocated with a circular point indicating the limit (maximum number of) allowed within the virtual data center.
- A bar chart showing the total number of virtual machine Storage (GB) allocated with a circular point indicating the limit (maximum number of physical servers) allowed within the virtual data center.

Modifying the Shared Server Zone

Note You must be a Cloud Provider Technical Administrator to perform this action.

Modify the attributes for the data center zone, which include provisioning networks and the vCenter data center, in which all Cloud servers are deployed.

Step 1 Choose **My Workspace** from the module drop-down list and then click the **System Setup** tab.

Step 2 On the System Setup portal click **Shared Zone**.

Figure 3-21 Shared Zone Portlet

Step 3 On the Shared Zone portlet, click **Modify a Shared Zone**.

Step 4 On the Create a Shared Server Zone form, specify the following information:

Table 3-2 .Shared Zone Details

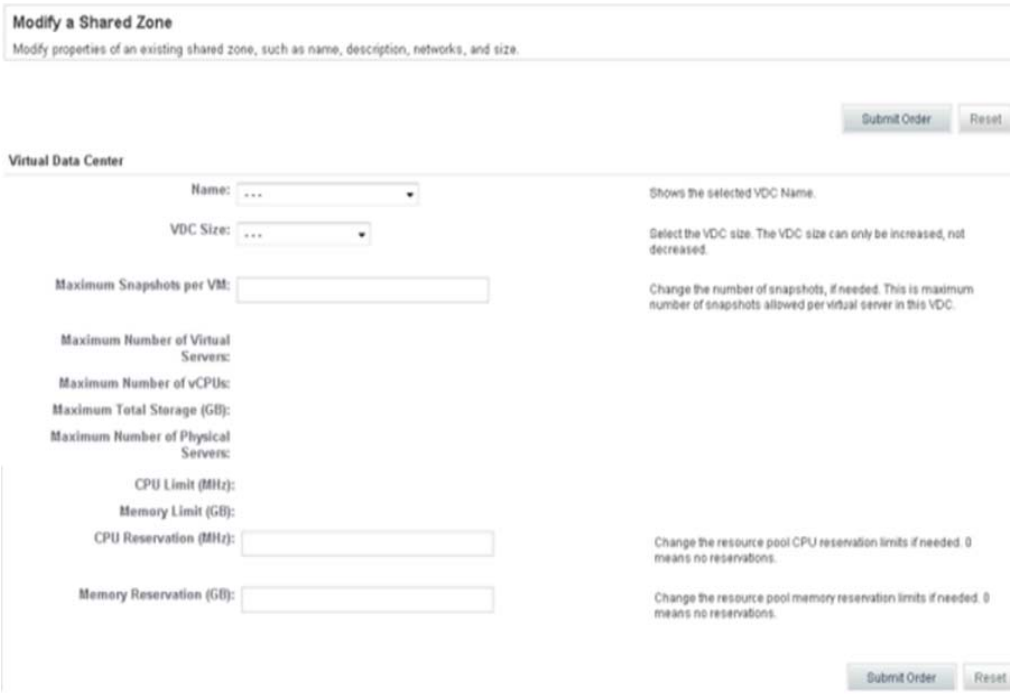
Field	Action
VDC Size	Select the size of the shared zone. The size determines the maximum limits for the number of virtual servers, vCPUs, CPU MHz, memory, and storage. The sizes can only be increased and not decreased.
Maximum Snapshots per VM	Modify the maximum snapshots per VM if needed.This limits the maximum number of snapshots allowed per virtual server.
Maximum Virtual Machines	Read-only field determined by the VDC size selected. This limits the maximum number of virtual server allowed in the virtual data center.
Maximum Total VM CPUs	Read-only field determined by the VDC size selected. This limits the maximum number of vCPUs allowed in the virtual data center. The number of vCPUs is determined based on the server size for the virtual server.

Field	Action
CPU limit (MHz)	Read-only field determined by the VDC size selected. A VMware resource pool is created with CPU limit size (MHz) limit defined for the VDC size.
Maximum Total VM Storage (GB)	Read-only field determined by the VDC size selected. This limits the maximum amount of storage utilization allowed in the virtual data center. The amount of storage used is determined based on the server size for the virtual server.
Maximum Total VM Memory (GB)	Read-only field determined by the VDC size selected. This limits the maximum amount of memory utilization allowed in the virtual data center. The amount of memory used is determined based on the server size for the virtual server.
Maximum Physical Servers	Read-only field determined by the VDC size selected. This limits the maximum number of physical servers allowed in the virtual data center.
Memory Limit (GB)	Read-only field that shows the Memory Limit in MHz for the resource pool. This is based on the VDC Size selected. This corresponds directly to the VMware resource pool Memory Limit.
CPU Reservation (MHz)	Enter the CPU reservation in MHz for the virtual data center resource pool. The default value is based on the VDC Size selected. This corresponds directly to the VMware resource pool CPU reservation.
Memory Reservation	Enter the memory reservation in GB for the virtual data center resource pool. The default value is based on the VDC Size selected. This corresponds directly to the VMware resource pool memory reservation

Step 5 If needed, edit the vCenter path in the VMware vCenter data center field.

Caution **For Cisco Intelligent Automation for Cloud 3.1.1, vCenter object names cannot contain forward slashes**. For more information, *see* the VMware software preparation prerequisites in the *Cisco Intelligent Automation for Cloud 3.1.1 Configuration Guide*.

Figure 3-22 Modify Shared Server Zone Form



Step 6 Click **Submit Order**.

Managing Power on Physical Servers

Powering Down a Physical Server

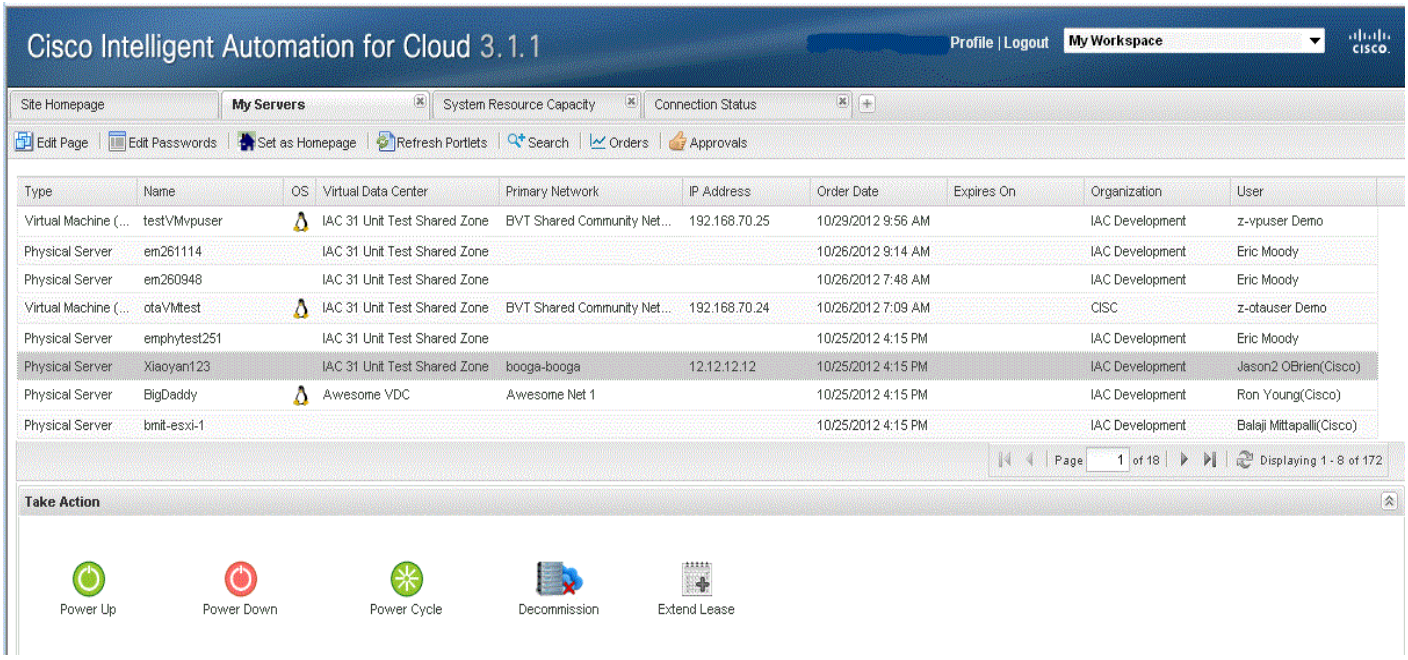
Power down an active physical server, regardless of its operating system state.

Note For information on removing a physical server from use, see Decommissioning a Physical Server, page 2-10.

Step 1 Choose **My Workspace** from the module drop-down list and then click the **My Servers** tab.

Step 2 On the My Servers portal (Figure 3-7 on page 3-13), locate and click the physical server that you want to power down.

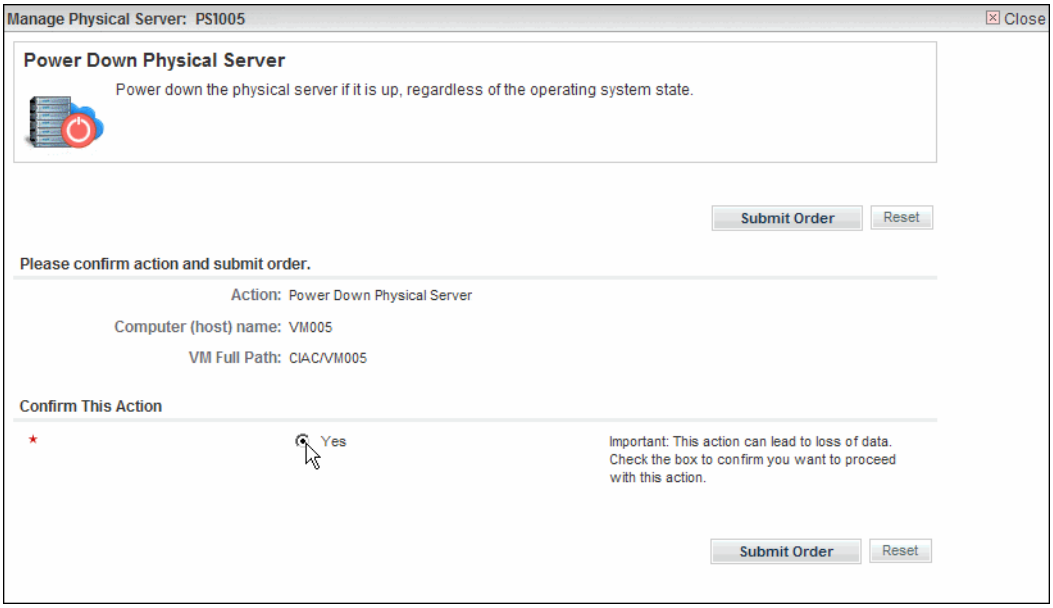
Figure 3-23 Power Down Physical Server



Step 3 In the Take Action panel, click the **Power Down** icon.

The Power Down Physical Machine form displays the name of the server.

Figure 3-24 Power Down Physical Form



Step 4 In the Confirm Action area, check the check box if you are sure the selected server is the one that you want to power down.

Step 5 Click **Submit Order**.

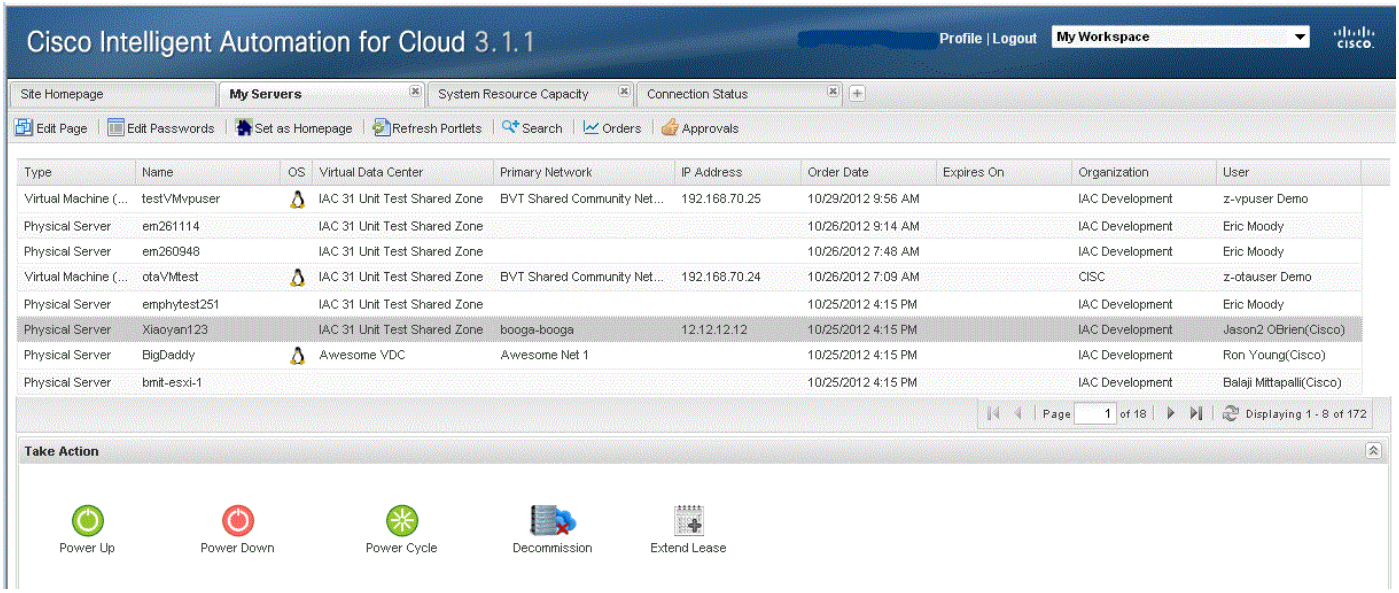
Power-cycling a Physical Server

Use the power-cycle service to reset power on a physical server.

Step 1 Choose **My Workspace** from the module drop-down list and then click the **My Servers** tab.

Step 2 On the My Servers portal (Figure 3-7 on page 3-13), locate and click the physical server that you want to power cycle.

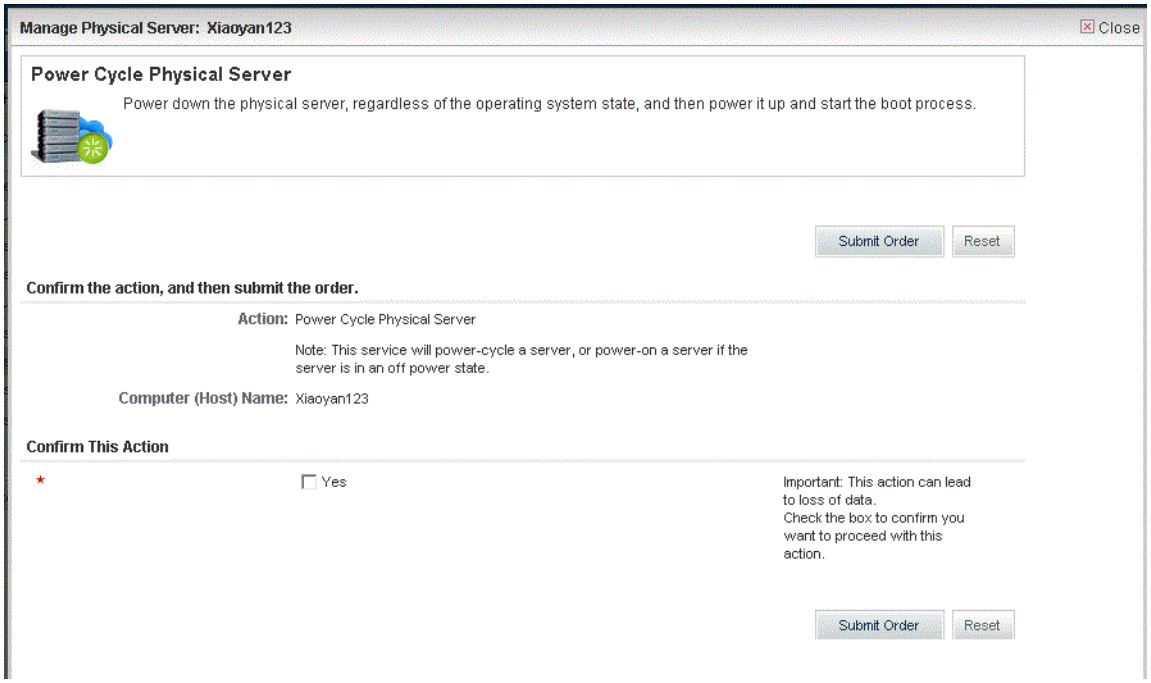
Figure 3-25 Power Cycle Physical Server



Step 3 In the Take Action panel, click the **Power Cycle** icon.

The Power Cycle Physical Machine form displays the name of the server.

Figure 3-26 Power Cycle Physical Form



Step 4 In the Confirm Action area, check the check box if you are sure the selected server is the one that you want to power cycle.

Step 5 Click **Submit Order**.

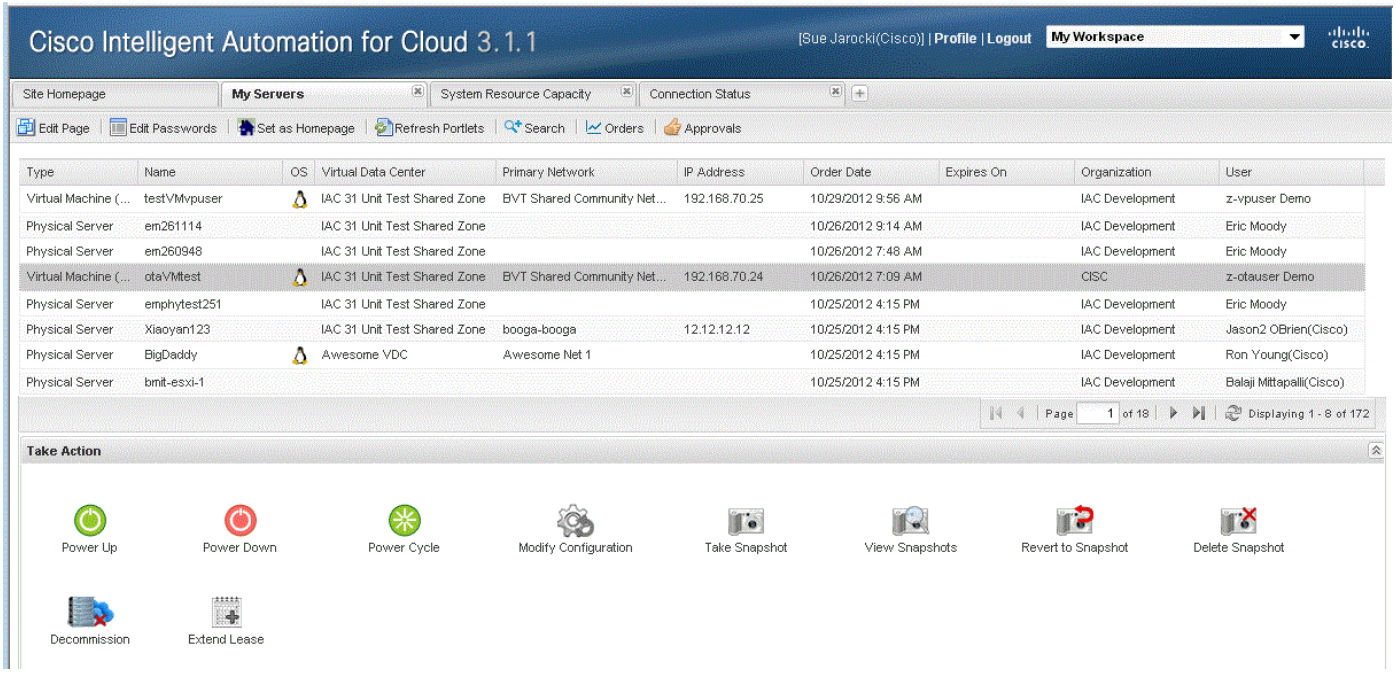
Powering Up a Physical Server

Power up a physical server and start the boot process.

Step 1 Choose **My Workspace** from the module drop-down list and then click the **My Servers** tab.

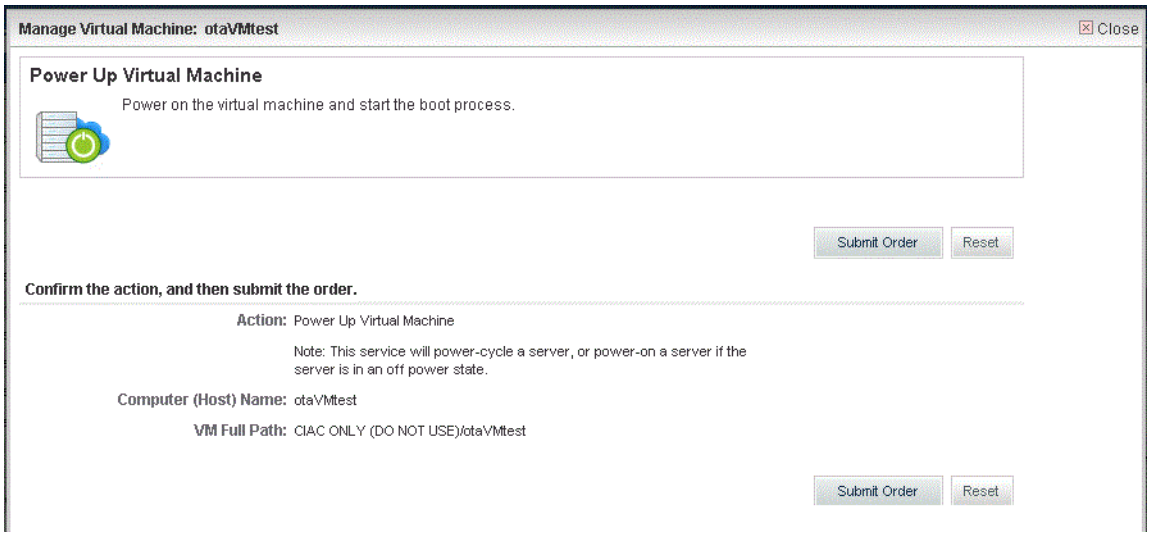
Step 2 On the My Servers portal (Figure 3-7 on page 3-13), locate and click the physical server that you want to power up.

Figure 3-27 Power Up Physical Server



Step 3 In the Take Action panel, click the **Power Up** icon.

Figure 3-28 Power Up Physical Form



Step 4 Click **Submit Order**.

Managing Cisco UCS Blades and Blade Pools

Note Only Cloud Provider Technical Administrators can transition blades between pools or remove blades.

When a blade is first registered, it is placed into the Maintenance pool in the Available state. After registration, the Cloud Provider Technical Administrator manages blades using the Manage Pools and Remove UCS Blade services.

There are three pool types:

- Maintenance—A holding area for blades that are registered but have not been indentified 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.

Registering a UCS Blade

The Cloud Portal Technical Administrator can register a discovered UCS Blade in the cloud system for users to select when ordering physical servers. The blade can be in Discovered, Maintenance, or Ignored states to change it to Registered.

Note Before you can register a UCS Blade, it must be discovered using the CloudSync Infrastructure Discovery portal.

To register a UCS Blade:

Step 1 Choose **My Workspace** from the module drop-down list, then click **Manage Cloud Infrastructure**.

Step 2 Click the **UCS Blades** icon.

Step 3 Select the line item you wish to register in the grid, then click the **Register** button.

Step 4 Click **Submit Order**.

Managing Blade Pools

For information about managing blade pools, see Chapter 8, Post-Configuration Options in the *Cisco Intelligent Automation for Cloud 3.1.1Configuration Guide*.

Managing Networks

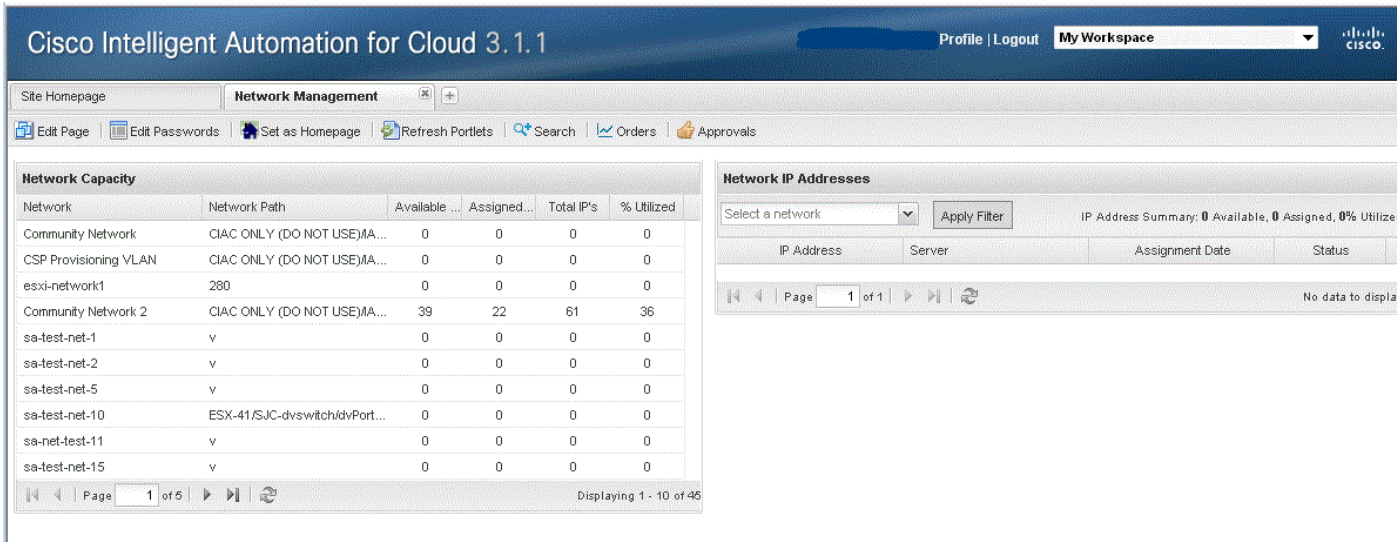
View, add, modify, and remove the following types of networks that exist in the cloud system.

Viewing the List of All Networks

To view a list of your networks and IP capacity information for each network, choose **My Workspace** from the module drop-down list and then click the **Network Management** tab.

On the Network Management portal the My Network IP Addresses panel lists your networks. The Network Capacity panel displays capacity information for available, assigned, and utilized IPs.

Figure 3-29 Network Management Portal



Viewing the list of a Specific Network

Sometimes you'd like to view only IP capacity information for a specific retwork rather than for all available networks.

Step 1 Select a network like usertest.

Step 2 Click refresh..

Step 3 The Network Capacity panel displays capacity information from other networks

Step 4 In order to see only IPs for usertest, click Apply filter.

Modifying Properties of a Network

You can use the modify network properties to reassign a layer 3 (IP) network to a different set of underlying layer 2 networks such as UCS vlans and VMware portgroups.

Modify the layer 2 attributes of an IP network, including VLAN and port group.

Step 1 Choose **My Workspace** from the module drop-down list and then click the **System Setup** tab.

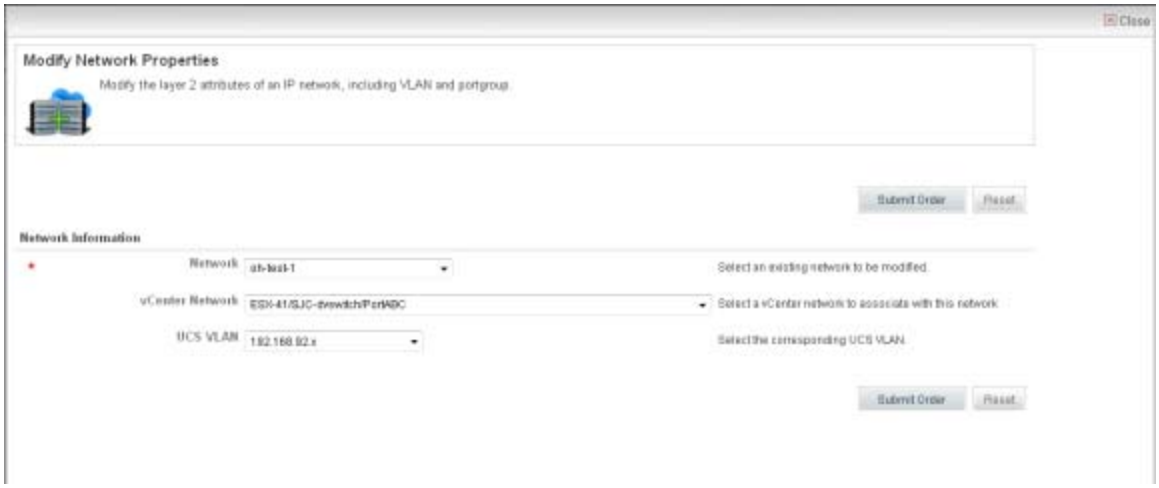
Step 2 On the **System Setup** portal, click on the **Networks** tab and then click on **Modify Network Properties**.

Step 3 Select the **Network** you want to be modified.

Step 4 Select the **vCenter Network** that you want to associate with the network.

Step 5 Select the corresponding **UCS VLAN** instance that you want to associate with the network.

Figure 3-30 Modify Network Properties



Step 6 Click **Submit Order**.

Adding a Network

For information about adding an infrastructure, community, user, or management network, see Chapter 8, Post-Configuration Options, in the *Cisco Intelligent Automation for Cloud Configuration Guide*.

Add a Network to a Shared Zone

After a Shared Zone is provisioned, additional networks can be added. Since shared zones are a community virtual center, networks are added to the shared zone through the My Virtual Data Centers portal page. The network to be added must already exist. To add additional networks see For information about adding an infrastructure, community, user, or management network, see Chapter 8, Post-Configuration Options, in the Cisco Intelligent Automation for Cloud Configuration Guide., page 3-40. Only community networks can be added to the Shared Zone.

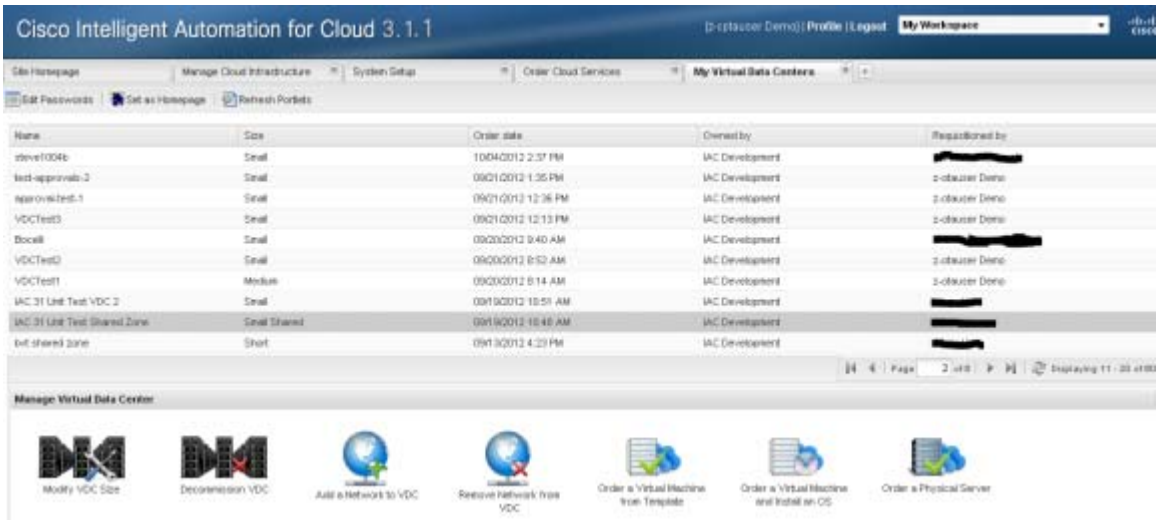
Note You must be a Cloud Provider Technical Administrator for Add a Network to a Shared Zone.

To add a network to the shared zone:

Step 1 Choose **My Workspace** from the module drop-down list and click the **My Virtual Data Centers** tab.

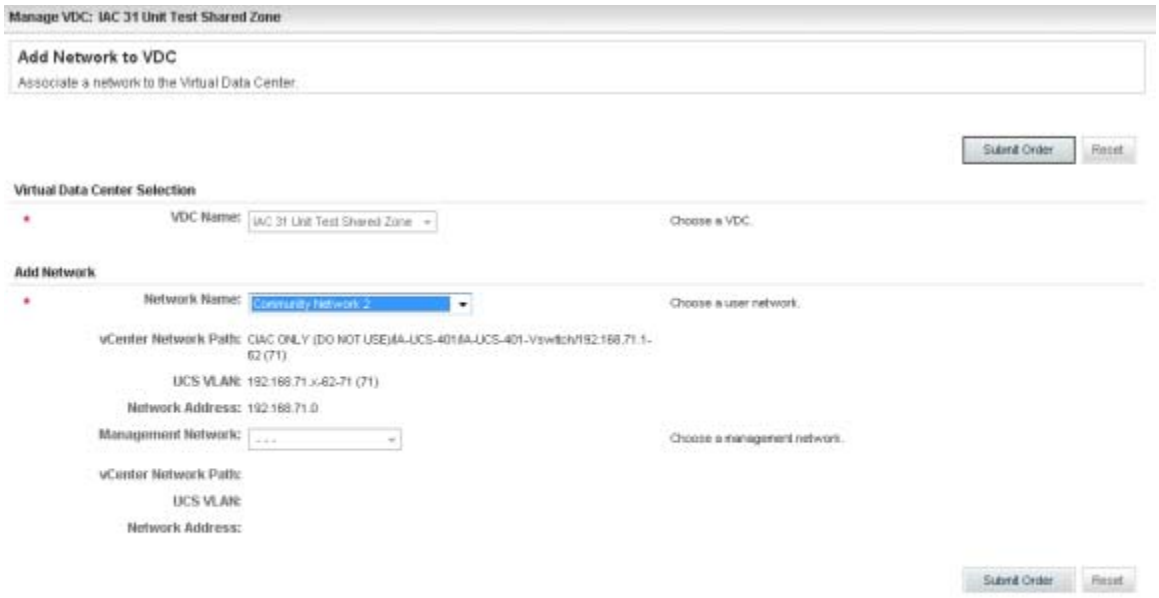
Step 2 Select the Shared Zone in the list of virtual data centers that a network should be added to.

Figure 3-31 Add Network to Shared Zone Portal.



Step 3 Click the **Add Network to VDC** action.

Figure 3-32 Add Network to VDC Form



Step 4 In the Network Name field, select the network to be added. Only community networks are shown.

Step 5 In the Management Network field, optionally select a management network to be associated with the community network. The management network should be the same subnet size as the community network.

Add Network to Virtual Data Center

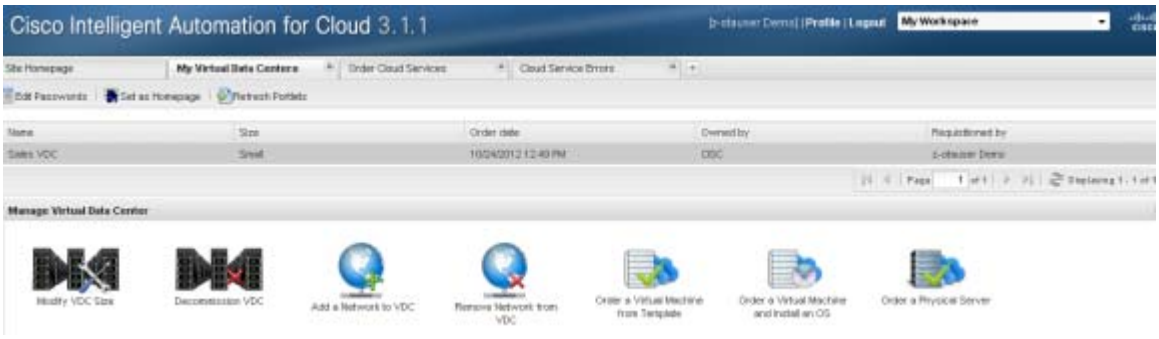
After a virtual data center is created, Organization Technical Administrators can request additional networks for the virtual data center. Once the request is submitted, the Cloud Portal Technical Administrator must approve the request and assign a new network to the virtual data center. The network to be added must already exist. To add additional networks see For information about adding an infrastructure, community, user, or management network, see Chapter 8, Post-Configuration Options, in the Cisco Intelligent Automation for Cloud Configuration Guide., page 3-40.

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:

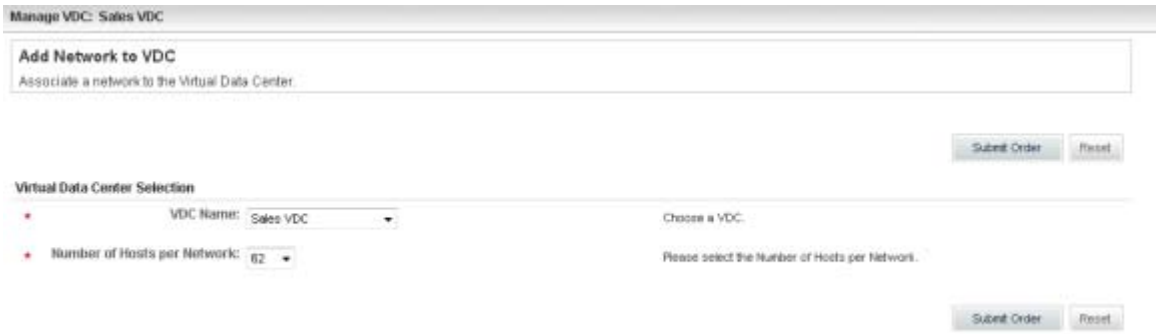
Step 1 Choose **My Workspace** from the module drop-down list and click the **My Virtual Data Centers** tab.

Figure 3-33 Add Network to VDC



Step 2 Click the **Add Network to VDC** action.

Figure 3-34 Add Network to VDC Form



Step 3 Select 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.

Step 4 Click **Submit Order**. The requisition will go to the Cloud Provider Technical Administrator for approval.

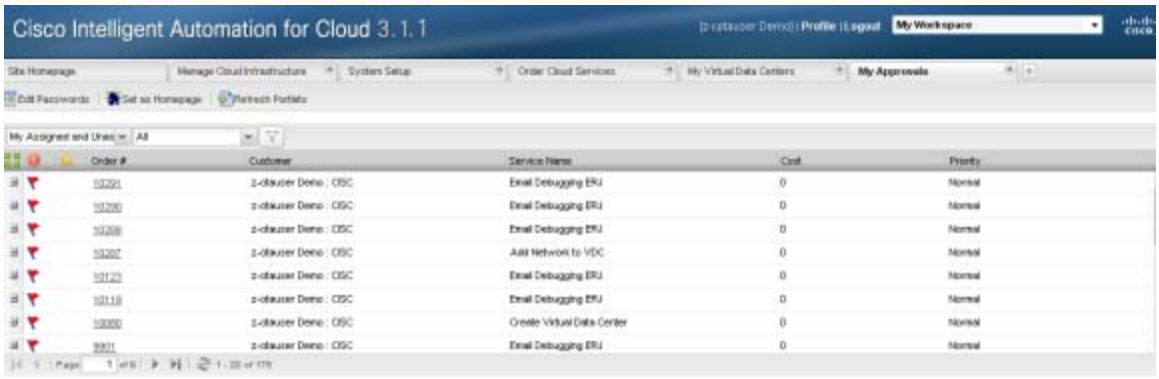
Approvals for Add Network to VDC

Note You must be a Cloud Provider Technical Administrator for Add Network to VDC approvals.

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.

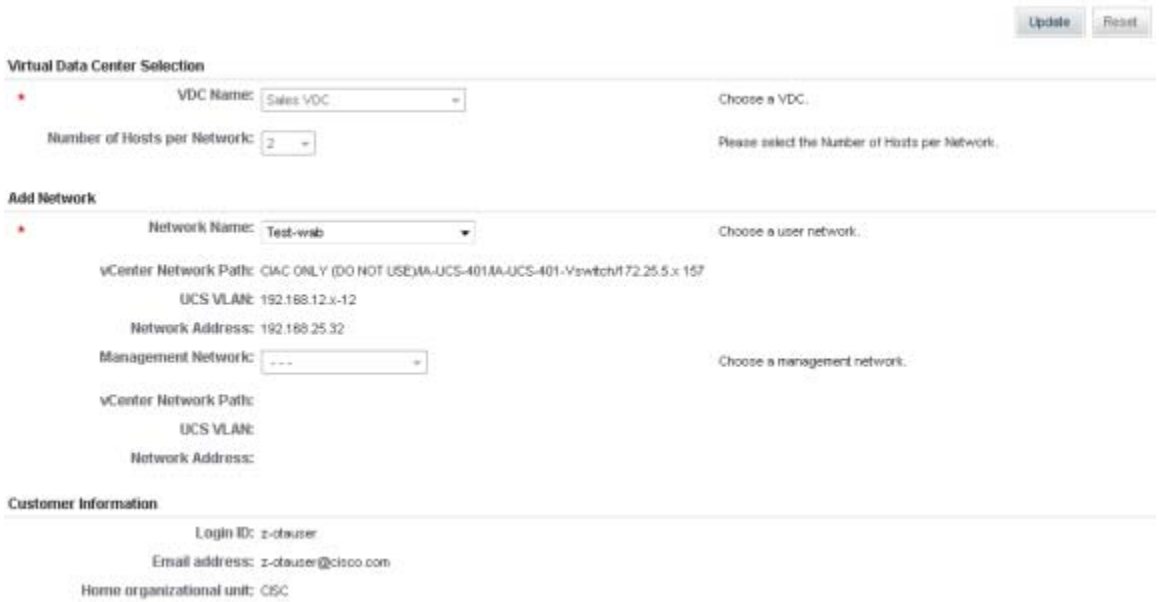
Step 1 Choose **My Workspace** from the module drop-down list and click the **My Approvals** tab.

Figure 3-35 Add Network to VDC Approval Portal



Step 2 Click on the **Order #** for the Add Network to VDC requisition that requires approval. This brings up the requisition.

Figure 3-36 Add Network to VDC Approval



Step 3 In the Network Name field, select the network to be added.

Step 4 In the Management Network field, optionally select a management network to be associated with the community network. The management network should be the same subnet size as the community network.

Step 5 Click **Update** to update the requisition with the VDC resource assignment information.

Step 6 Click **Approve** for the request.

Deleting a Network from the Cloud System

Permanently remove a network.

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

Step 1 Choose **My Workspace** from the module drop-down list and then click the **System Setup** tab.

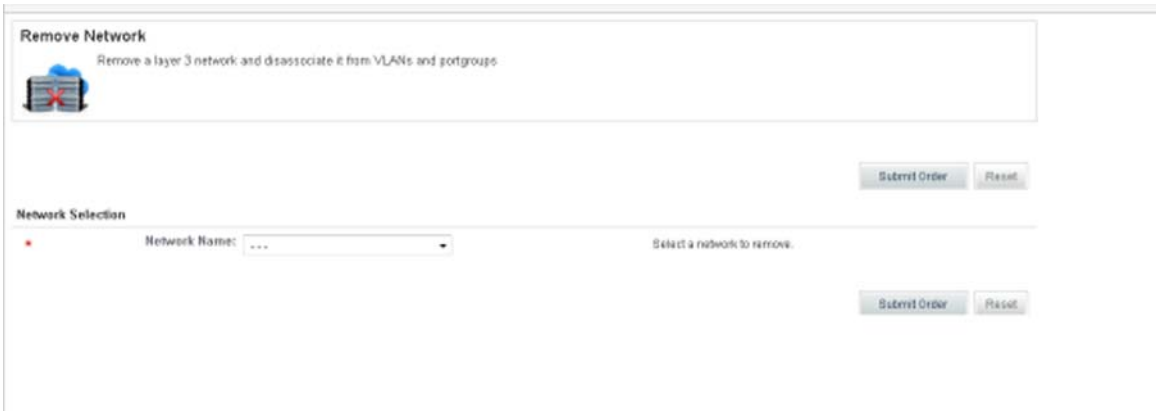
Step 2 On the System Setup portal click the **Networks** tab.

Step 3 On the Networks portlet, click **Remove Network**.

Step 4 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.

Figure 3-37 Remove Network Form



Step 5 Click **Submit Order**.

Managing IP Address Exclusions

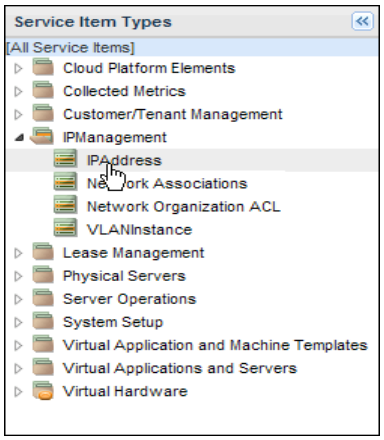
Add or remove a usage exclusion for an IP address.

When an IP address in 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 Cloud portal.

Step 1 Choose **Service Item Manager** from the module drop-down list and then click the **Manage Service Items** tab.

Step 2 On the Manage Service Items tab (Figure 1-8 on page 1-9), expand IP Management in the Service Items Type panel, then click **IPAddress**.

Figure 3-38 Service Item Type—IPAddress

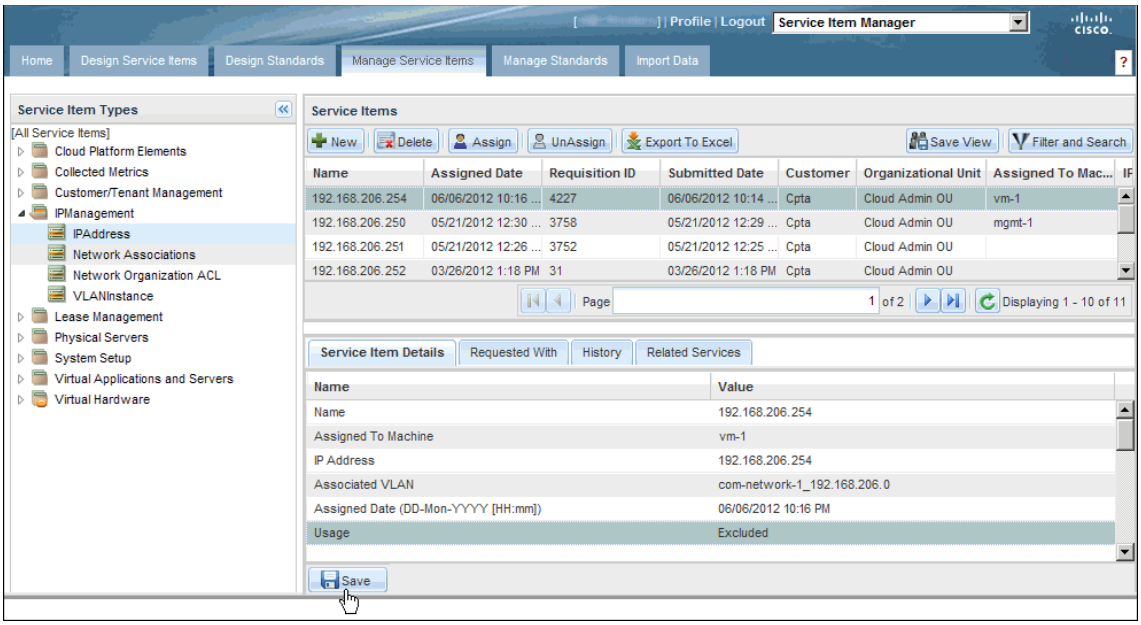


Step 3 Locate and click the IP address in the Service Items table.

Step 4 Click in the Usage field and change the value to one of the following values:

- Excluded—Apply the exclusion
- Unassigned—Remove an existing exclusion

Figure 3-39 IP Address—Exclusion



Step 5 Click **Save**.

Removing a Network from a Virtual Data Center

Note You must be a Cloud Provider Technical Administrator or an Organization Technical Administrator to perform this action.

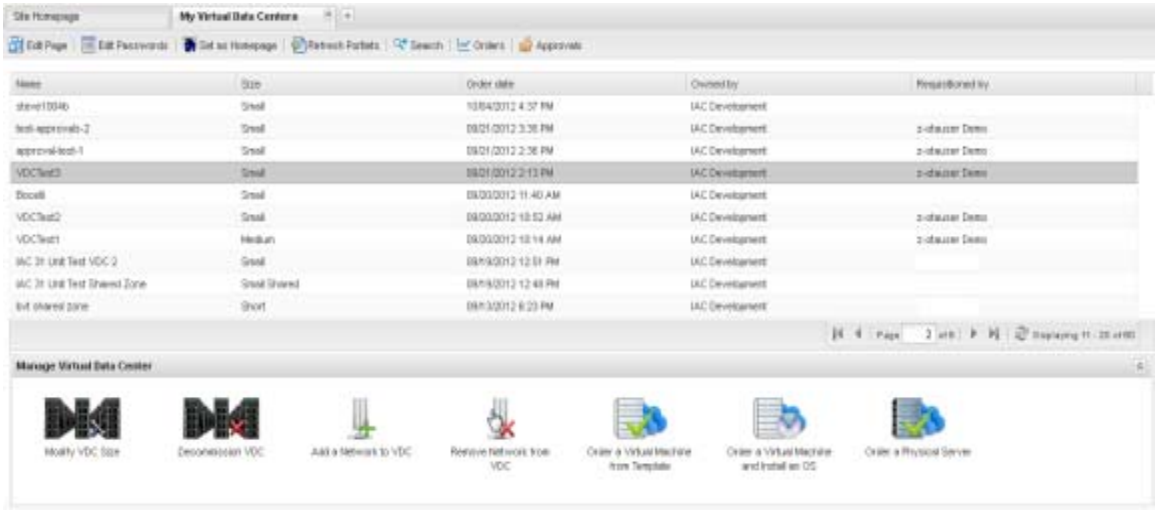
Note If a virtual data center does not have an associated network the Remove Network from VDC button will be greyed-out and not clickable.

Step 1 In Cloud Portal, choose **My Workspace** from the module drop-down list, then click on **My Virtual Data Centers**.

Step 2 Locate the virtual data center in the grid, then click the name.

Step 3 In the Manage Virtual Data Center collapsible panel, click on **Remove Network from VDC**.

Figure 3-40 Remove Network



Step 4 Select the network you want to remove from the **Network Name** drop down list.

Step 5 Click **Submit Order**.

Managing Server Templates

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

- Virtual machine (VM) template (see Managing Virtual Machine Templates, page 3-48)
- Operating system from Cisco Server Provisioner (see Managing Operating System Templates, page 3-53)
- UCS service profile template (see Managing UCS Service Profile Templates, page 3-54)
- Email notification templates (see Managing Email Notification Templates, page 3-55)
- Authorization and review escalation (see Managing Authorization and Review Escalation, page 3-59

Virtual machine, operating system, andUCS service profile templates are discovered and registered using the CloudSync Infrastructure Discovery portal. See Managing Cloud Infrastructure Discovery, page 3-3. The state transitions included are shown in Table 3-1Allowed Discovered State Transitions, page 3-7.

After registering, the templates are then uniformly available to all users.

Managing Virtual Machine Templates

Use the instructions in this section to manage your virtual machine templates:

- Converting a Virtual Machine to a Template, page 3-49
- Cloning a Virtual Machine as a Template, page 3-51
- Registering a Virtual Machine Template, page 3-52
- Maintaining a Virtual Machine Template, page 3-52
- Ignoring a Virtual Machine Template, page 3-53

Converting a Virtual Machine to a Template

The Cloud Portal Technical Administrator can convert an existing virtual machine to a virtual machine template.

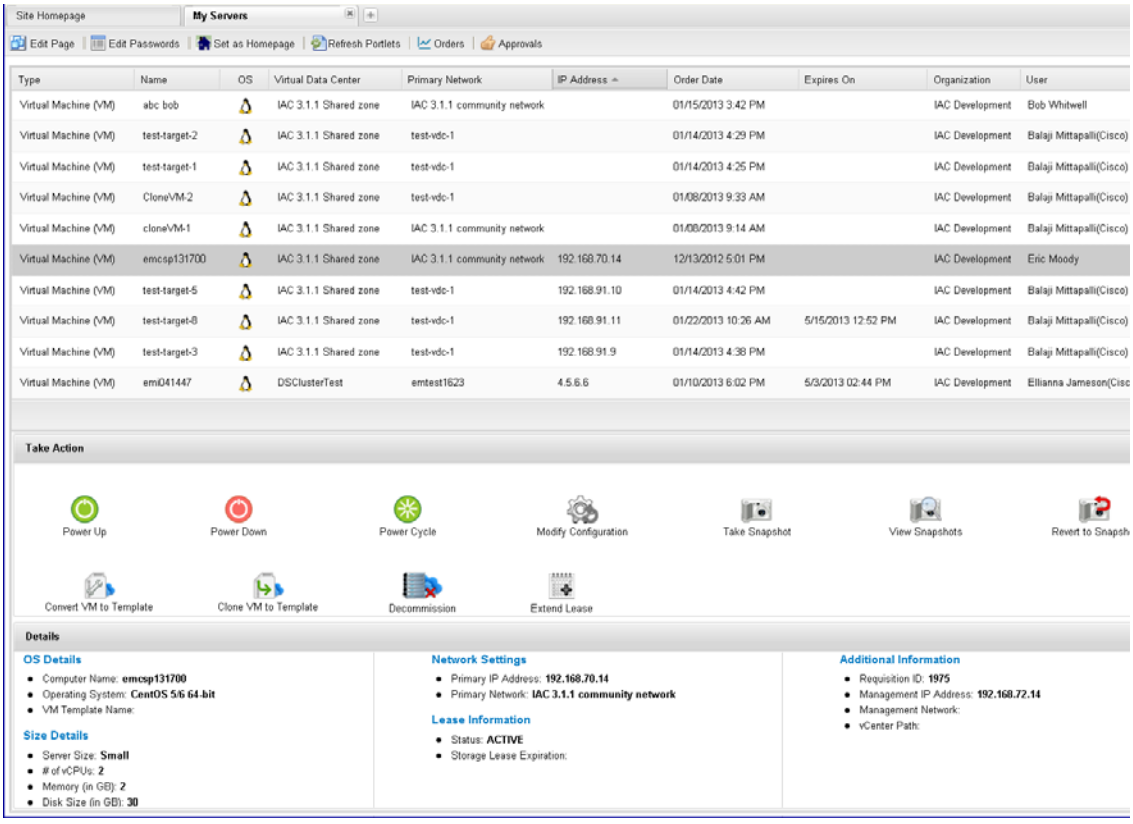
Caution If you convert a VM to a VM template, that VM will no longer be available for any further usage.

To convert a VM to a VM template:

Step 1 Open the My Servers portlet.

Step 2 In the list of servers, select the VM you'd like to convert to a VM template.

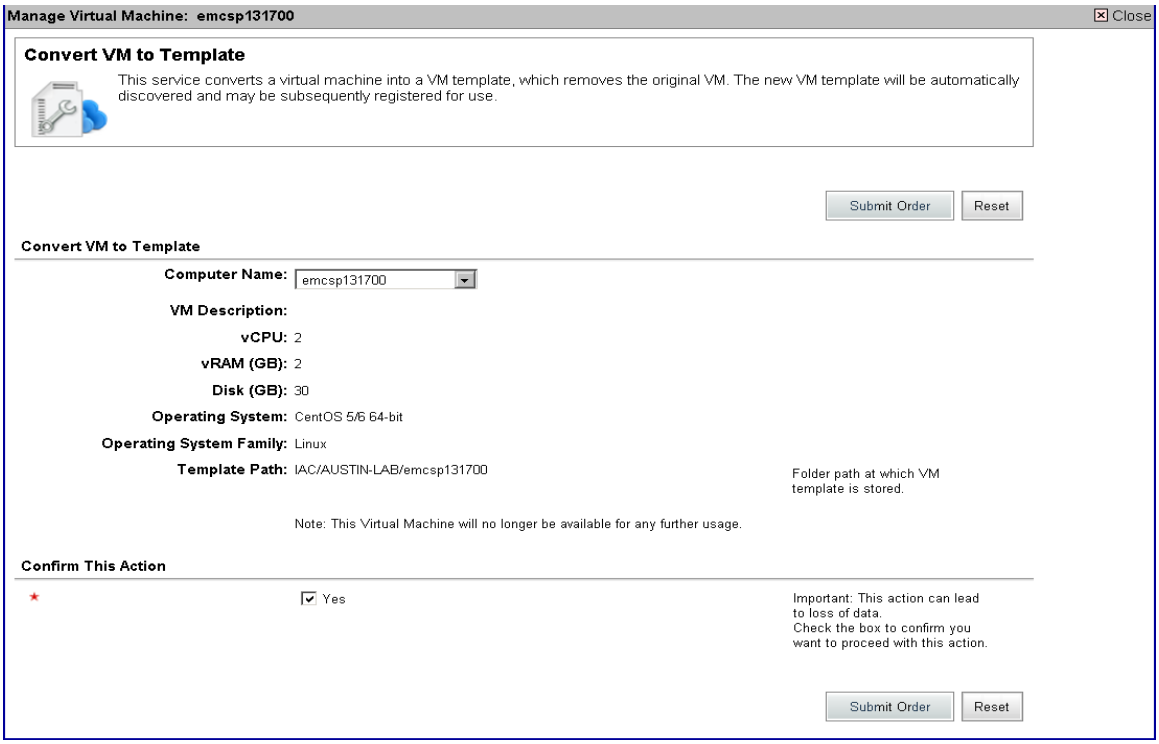
Figure 3-41 My Servers portlet



Step 3 Click the Convert VM to Template icon.

Step 4 Cisco IAC displays the **Convert VM to Template** form.

Figure 3-42 Convert VM to Template form



Step 5 Verify that this is the VM that you want to convert to a VM template.

Step 6 Check the **Confirm This Action** checkbox to acknowledge that data may be lost.

Step 7 Click **Submit Order**.

Cloning a Virtual Machine as a Template

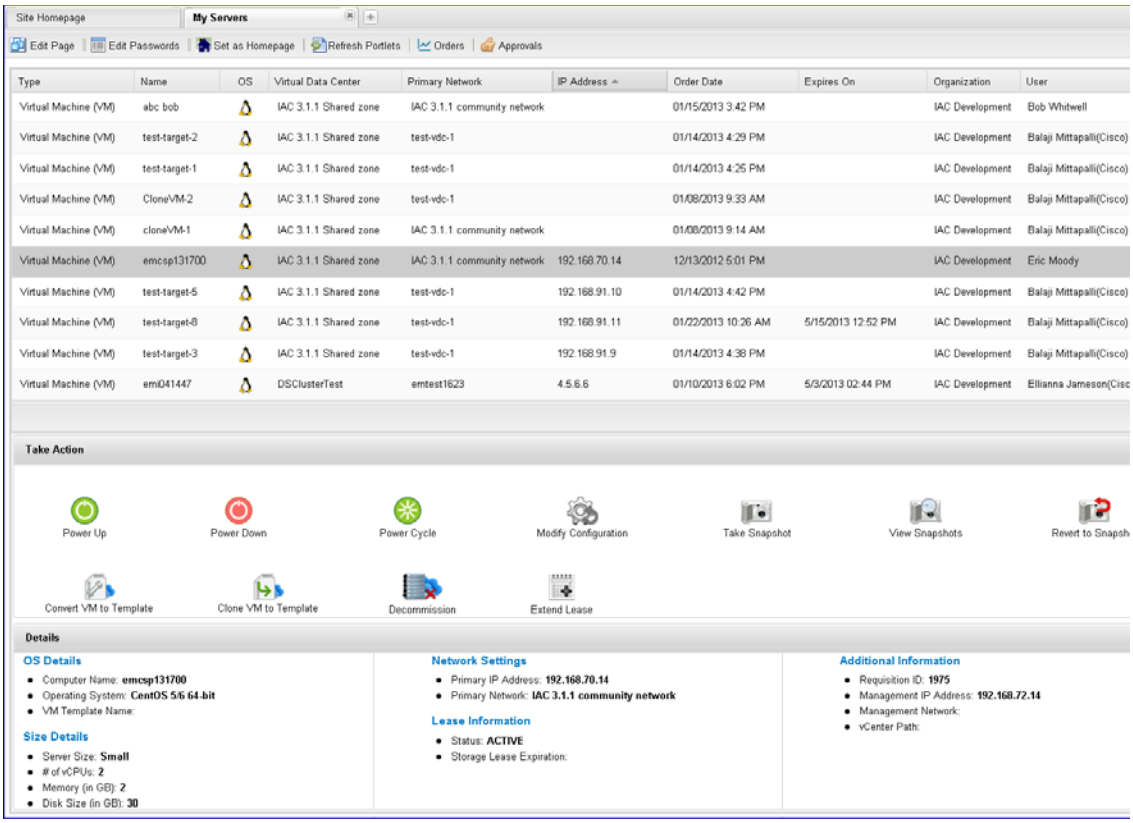
The Cloud Portal Technical Administrator can create a virtual machine template by cloning an existing virtual machine.

To clone a VM as a VM template:

Step 1 Open the My Servers portlet.

Step 2 In the list of servers, select the VM you'd like to clone to a VM template.

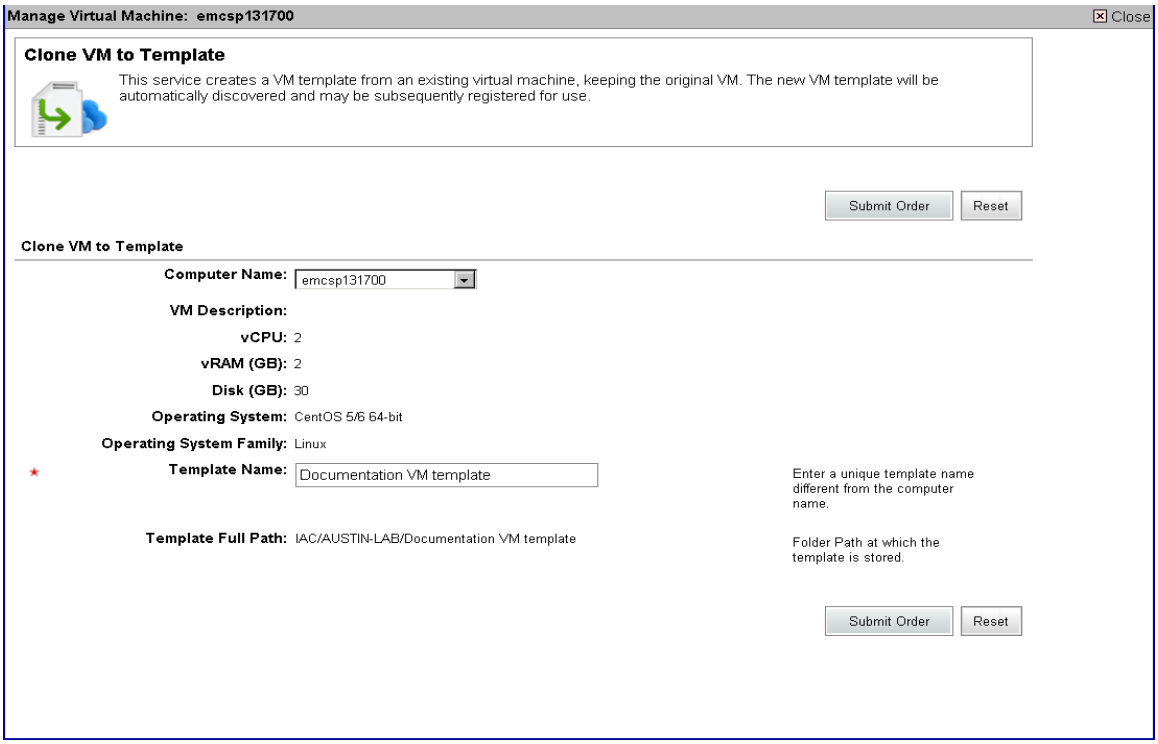
Figure 3-43 My Servers portlet



Step 3 Click the **Clone VM to Template** icon.

Step 4 Cisco IAC displays the **Clone VM to Template** form.

Figure 3-44 Clone VM to Template form



Step 5 Verify that this is the VM that you want to clone as a VM template.

Step 6 Click **Submit Order**.

Registering a Virtual Machine Template

For information about registering virtual machine templates, see Chapter 8, Post-Configuration Options, in the *Cisco Intelligent Automation for Cloud Configuration Guide*.

Maintaining a Virtual Machine Template

The Cloud Portal Technical Administrator can change the state of a VM Template to Maintenance to keep the template ready, but not be used for new servers within the Cisco IAC system.

Note The template must be in Registered state to set it to Maintenance.

To set the VM template to maintenance when already registered:

Step 1 Choose **My Workspace** from the module drop-down list and then click **Manage Cloud Infrastructure**

Step 2 Click the **VM Templates** icon.

Step 3 Select the line item you wish to set to **Maintenance** in the grid, and select the **Maintenance** button.

Step 4 Click **Submit Order**.

Ignoring a Virtual Machine Template

The Cloud Portal Technical Administrator can change the state of a VM 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 VM Template to Ignored:

Step 1 Choose My Workspace from the module drop-down list and then click Manage Cloud Infrastructure.

Step 2 Click the VM Templates icon.

Step 3 Select the line item you wish to set to Ignored in the grid, and select the Ignore button.

Step 4 Click Submit Order.

Managing Operating System Templates

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

- Registering an Operating System Template, page 3-53
- Maintaining an Operating System Template, page 3-53
- Ignoring an Operating System Template, page 3-54

Registering an Operating System Template

For information about registering operating system templates, see Chapter 8, Post-Configuration Options, in the *Cisco Intelligent Automation for Cloud Configuration Guide*.

Maintaining an Operating System Template

The Cloud Portal 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:

Step 1 Choose **My Workspace** from the module drop-down list and then click **Manage Cloud Infrastructure**.

Step 2 Click the **OS Templates** icon.

Step 3 Select the line item you wish to set to Maintenance in the grid, and select the **Maintenance** button.

Step 4 Click **Submit Order.**

Ignoring an Operating System Template

The Cloud Portal 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:

Step 1 Choose My Workspace from the module drop-down list and then click **Manage Cloud Infrastructure**.

Step 2 Click the **OS Templates** icon.

Step 3 Select the line item you wish to set to Ignored in the grid, and select the **Ignore** button.

Step 4 Click **Submit Order**.

Managing UCS Service Profile Templates

Use the instructions in this section to manage your UCS serviceprofile templates:

- Registering a UCS Service Profile Template, page 3-54
- Maintaining a UCS Service Profile Template, page 3-54
- Ignoring a UCS Service Profile Template, page 3-55

Registering a UCS Service Profile Template

For information about registering UCS service profile templates, see Chapter 8, Post-Configuration Options, in the *Cisco Intelligent Automation for Cloud Configuration Guide*.

Maintaining a UCS Service Profile Template

The Cloud Portal Technical Administrator can change the state of a UCS service profile 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 UCS service profile template to Maintenance when already Registered:

Step 1 Choose **My Workspace** from the module drop-down list and then click **Manage Cloud Infrastructure**.

Step 2 Click the **Service Profile Templates** icon.

Step 3 Select the line item you wish to set to Maintenance in the grid, and select the **Maintenance** button.

Step 4 Click **Submit Order**.

Ignoring a UCS Service Profile Template

The Cloud Portal 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.

To set the UCS service profile template to Ignored:

Step 1 Choose **My Workspace** from the module drop-down list and then click **Manage Cloud Infrastructure**.

Step 2 Click the **Service Profile Templates** icon.

Step 3 Select the line item you wish to set to **Ignored** in the grid, and select the **Ignore** button.

Step 4 Click **Submit Order**.

Step 5 Review the information to confirm that the selected operating system template is the one that you want to remove, then click **Submit Order**.

Managing Email Notification Templates

Use the instructions in this section to manage your email notification templates:

- Modifying Email Notification Templates, page 3-55
- Setting Return Email Address, page 3-59

Modifying Email Notification Templates

Cisco Intelligent Automation for Cloud 3.1 (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.

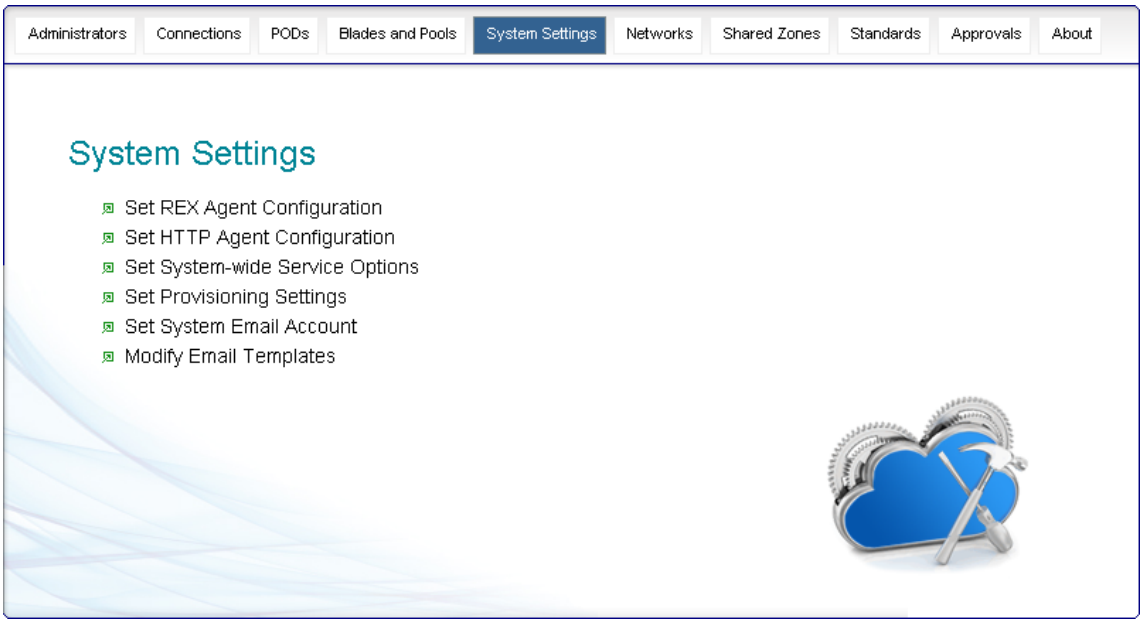
The email templates must be customized with the sender and recipient addresses. You can also optionally customize the subject and message.

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

Step 1 Choose **My Workspace** from the module drop-down list, then click the **System Setup** tab.

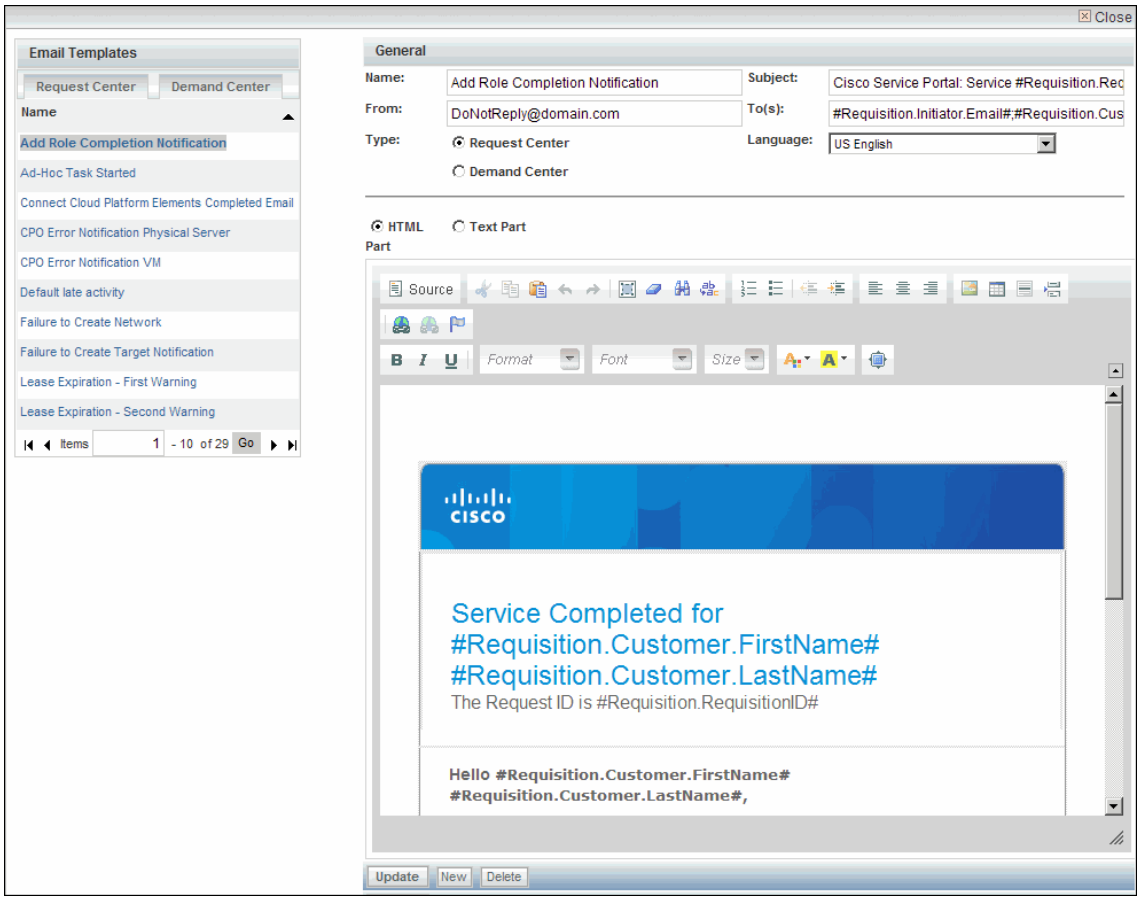
Step 2 On the System Setup portal page, click the **System Settings** tab to open the portlet.

Figure 3-45 System Settings Portlet



Step 3 On the System Settings portlet, click **Modify Email Templates** to open the form.

Figure 3-46 Email Templates Form



Step 4 On the Request Center tab in the Email Templates panel, click **Add Role Completion Notification** in the list.

Step 5 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)	Enter one or more valid recipient email addresses. For multiple recipients, separate email addresses using semi-colons. **Note** You can use namespace variables in this field. For information on using namespaces, *see* the *Cisco Service Portal Namespace Users Guide*. **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 does not have to be a real address, but it must be properly formatted (email@domain.com).

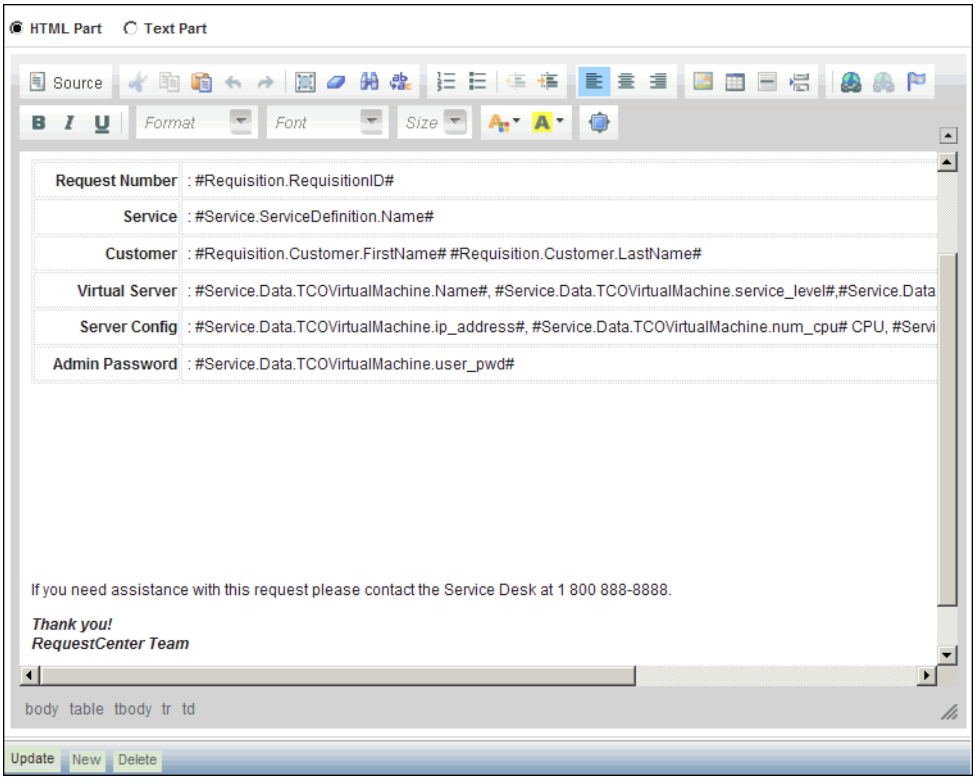
Field	Action
Language	Leave as is. In the current release, only US English is supported; any language selection you make will be ignored.
Type	Click the **Request Center** radio button.

Step 6 For the editing window, click one of the following radio buttons to choose an editor.

- **HTML Part** (shown in Figure 3-46 on page 3-57)
- **Text Part** (shown in Figure 3-47 on page 3-58)

Step 7 In the editing panel, modify default content and add optional content as needed.

Figure 3-47 Notification Template—Editing Panel



Step 8 Click **Update**.

Step 9 Repeat Step 4 through Step 8 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*.

Setting Return Email Address

To set a return email address, perform the following steps.

Step 1 Choose My Workspace from the module drop-down list and then click **System Setup** tab.

Step 2 In the System Set up portal page, click the **System Settings** tab to open the portlet.

Step 3 In the System Settings portlet, click **Set System Email Account**.

Step 4 Enter an actual, active email account with a valid SMTP format

Step 5 Click **Submit Order.**

Managing Authorization and Review Escalation

Use the instructions in this section to manage authorization and review escalation:

- Enabling an Authorization or Review, page 3-60
- Setting Up Escalation Sequences, page 3-61

Note You must be a Cloud Provider Technical Administrator to set up and modify authorizations.

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 the following organizations:

- Finance
- Departments
- Service groups

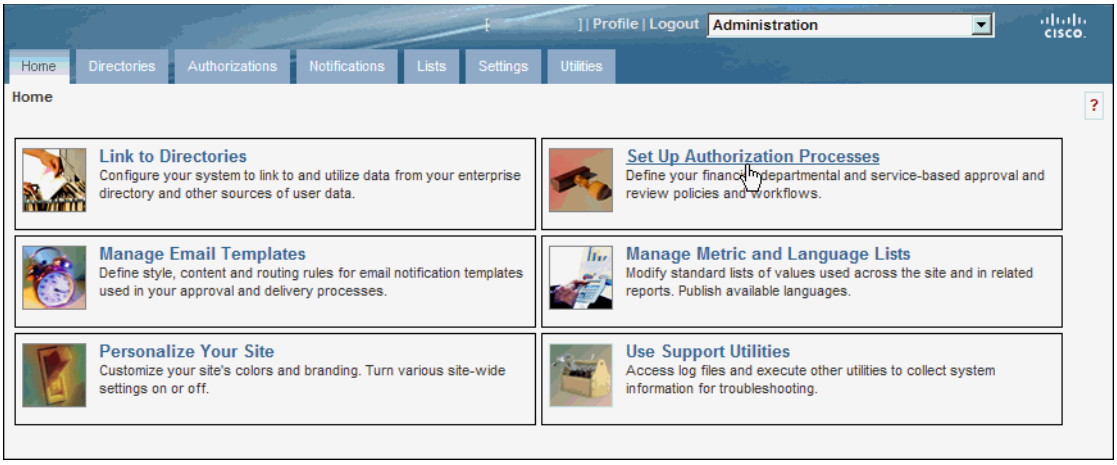
A review task requires the assigned reviewer to sign off on a step in the delivery process. Review sequences are configurable for the following organizations:

- Departments
- Service groups

Enabling an Authorization or Review

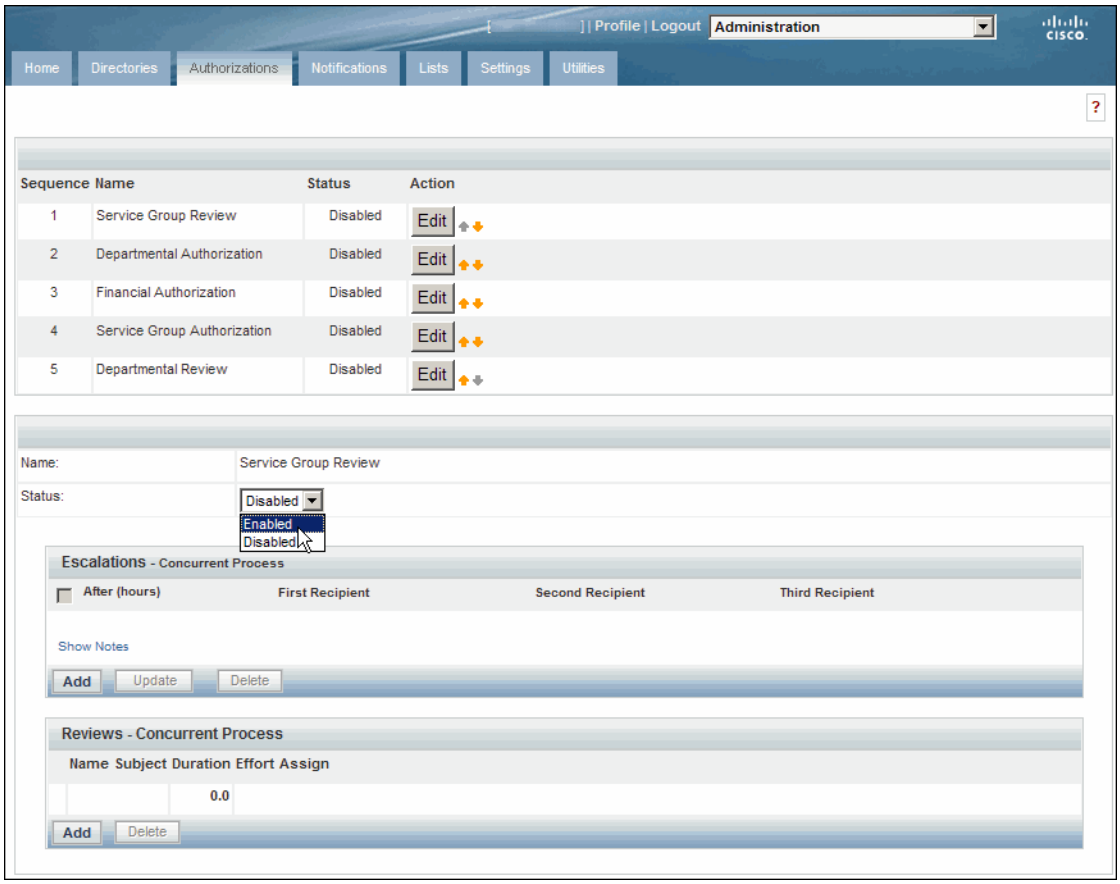
Step 1 Choose **Administration** from the module drop-down list and then click **Set Up Authorization Process**.

Figure 3-48 Administration Module—Set Up Authorization Processes



Step 2 Click **Edit** button next to Service Group Authorization.

Figure 3-49 Enabling Authorizations and Reviews



Step 3 Choose **Enabled** from the Status drop-down list.

Step 4 Repeat steps 2 and 3 if you need to enable any other Authorizations.

Setting Up Escalation Sequences

An escalation sequence is a series 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.

Step 1 Follow the steps outlined in Enabling an Authorization or Review, page 3-60.

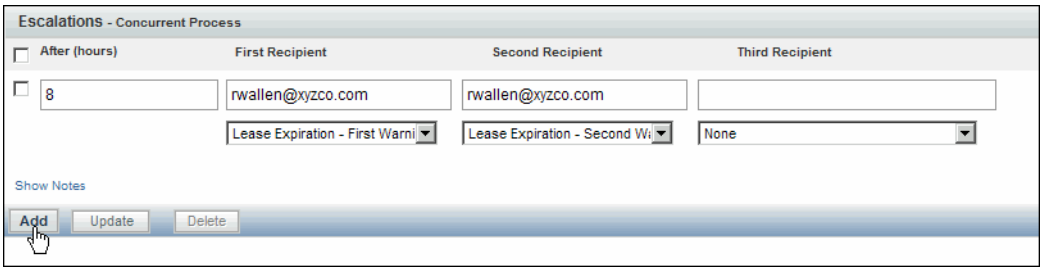
Step 2 Click **Edit** beside an authorization group in the list.

Note The asterisk * next to a field indicates that it is a required field and must contain a valid value.

Step 3 In the Escalations panel, click **Add**, then provide the following information:

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 3-55.

Figure 3-50 Adding an Escalation Sequence



CHAPTER 4

Managing Organizations and Users

Note If directory authorization has been enabled for your Cloud environment, then you may have to manage organizations and users from the directory rather than by using the Cloud Portal services outlined in this chapter. Directory integration can be configured so that organizations and users must be created, defined, and managed from the directory. In this case, any changes you make to an organization or user will be overridden by the definitions set in the directory. For more information, see Managing Organizations and Users With Directory Integration, page 4-2.

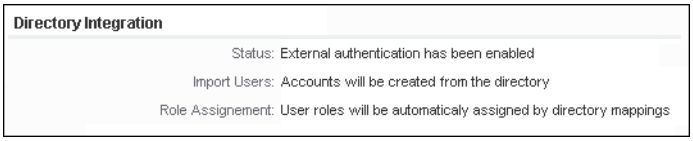
This chapter guides you through adding, configuring, and removing organizations and users. It includes the following sections:

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 Cloud Portal services described in this section. For instructions, see the documentation that came with your directory software.

If you are unsure whether directory integration is enabled in your Cloud environment, the information shown in Figure 4-1 will appear on the forms for adding, modifying, and removing users. If you see this information, it is strongly recommended that you do not proceed with the Cloud Portal service, because any changes you make will be overwritten by the directory service.

Figure 4-1 Directory Authorization Notation



Managing Organizations

Manage the user, management, and community networks within the cloud system that allow users to deploy cloud servers.

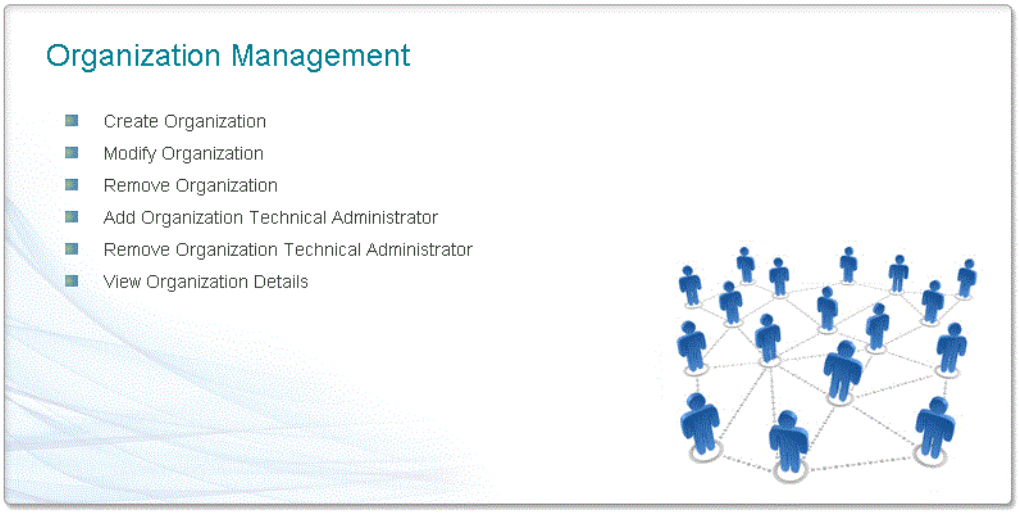
Note If directory authorization has been enabled for your Cloud environment, then you may have to manage organizations from the directory rather than by using the Cloud Portal services outlined in this section. Directory integration can be configured so that organizations must be created, defined, and managed from the directory. In this case, any changes you make to an organization will be overridden by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

Viewing Properties of an Organization

View details of an organization, such as number of users and lists of organization administrators and accessible networks/VLANs.

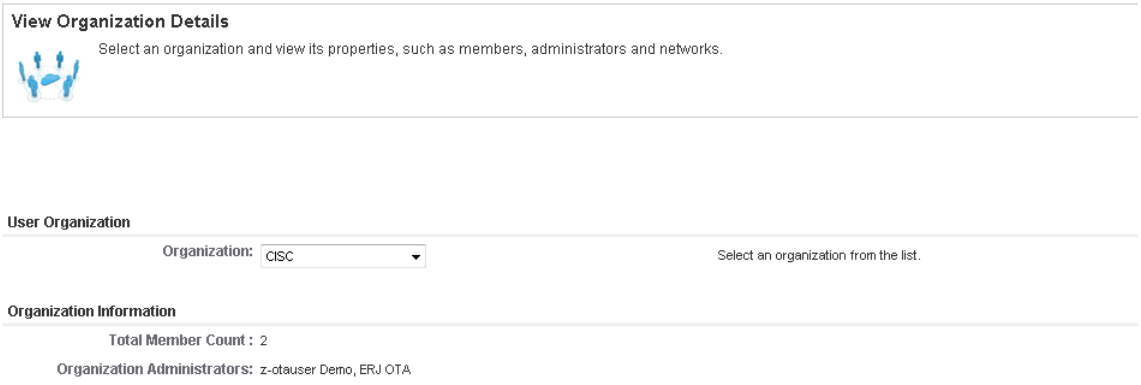
Step 1 Choose **My Workspace** from the module drop-down list and then click the **Organization Management** tab.

Figure 4-2 Organization Management Portal



Step 2 On the Organization Management portal click **View Organization Details**.

Figure 4-3 View Organization Details Form



Step 3 On the View Organization Details form, choose the organization from the drop-down list.

The number of members and designated Organization Technical Administrators are shown for the organization.

Creating an Organization

Define a new organization of Cloud users.

Note If directory authorization has been enabled for your Cloud environment, then you may have to create organizations from the directory rather than by using this Cloud Portal service. Directory integration can be configured so that organizations must be created, defined, and managed from the directory. In this

case, any changes you make to an organization or user will be overridden by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

Note To add an Organization Technical Administrator to the new organization, see Adding or Removing an Organization Technical Administrator, page 4-14.

Step 1 Choose **My Workspace** from the module drop-down list and then click the **Organization Management** tab.

Step 2 On the Organization Management portal (Figure 4-2 on page 4-3), click **Create Organization**.

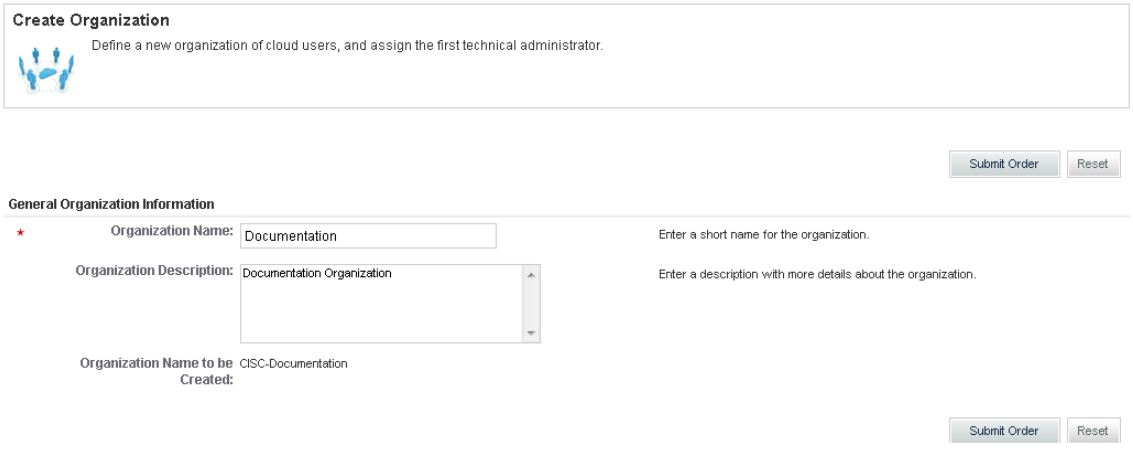
Step 3 On the Create Organization form, enter the following information.

Caution **For Intelligent Automation for Cloud 3.1 (IAC), vCenter object names cannot contain forward slashes**. For more information, *see* the VMware software preparation prerequisites in the *Cisco Intelligent Automation for Cloud 3.1 Configuration Guide*.

Note Fields marked with asterisks are required.

Field	Action
Organization Name	Enter a descriptive name for the organization.
Organization Description	*Optional.*
Organization Name to be Created	Read-only field showing the name of the organization to be created. The organization name is prepended with the cloud administration organization's company acronym.

Figure 4-4 Create Organization Form



Step 4 Click **Submit Order**.

Removing an Organization

Remove an organization from the cloud system.

Note If directory authorization has been enabled for your Cloud environment, then you may have to remove organizations from the directory rather than by using this Cloud Portal service. Directory integration can be configured so that organizations created, defined, and managed from the directory. In this case, any changes you make to an organization will be overridden by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

Note You can only remove an organization if the unit currently has no provisioned servers or virtual data centers. To decommission servers or virtual data centers, see Decommissioning a Physical Server, page 2-10, Decommissioning a Virtual Machine, page 2-6, and Decommissioning a Virtual Data Center, page 2-17.

Step 1 Choose **My Workspace** from the module drop-down list and then click the **Organization Management** tab.

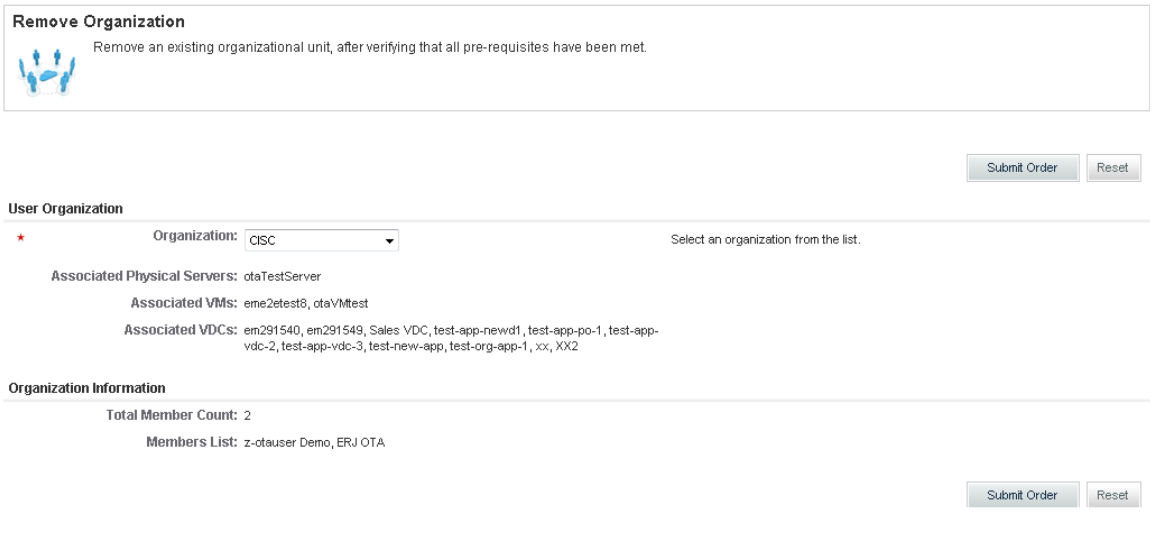
Step 2 On the Organization Management portal (Figure 4-2 on page 4-3), click **Remove Organization** to open the form.

Step 3 On the Remove Organization form (Figure 4-5 on page 4-5), choose the organization that you want to remove from the Organization Name drop-down list.

The associated physical servers, associated virtual machines, and virtual data centers are shown.

Step 4 Review the information to confirm that the selected organization is the one that you want to remove, then click **Submit Order**.

Figure 4-5 Remove Organization Form



Creating and Managing Users

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 Cloud Portal 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 a user using Cloud Portal will be overwritten by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

The following sections provide information and instructions for adding, modifying, and removing a user from an organization.

- Adding or Removing a Cloud Provider Technical Administrator, page 4-6
- Adding or Removing an Organization Technical Administrator, page 4-14
- Adding or Removing a Server Owner, page 4-20

Adding or Removing a Cloud Provider Technical Administrator

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 Cloud Portal 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 Cloud Portal will be overwritten by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

The following sections provider instructions for managing users in the Cloud Provider Technical Administrator role.

- Adding an Existing User as a Cloud Provider Technical Administrator, page 4-7—Assign the Cloud Provider Technical Administrator role to a user who has already been created in the Cloud system.
- Creating a New User to Add as a Cloud Provider Technical Administrator, page 4-10—Create a new user, then add the assign the Cloud Provider Technical Administrator role to the new user.
- Removing a Cloud Provider Technical Administrator, page 4-12—Remove a Cloud Provider Technical Administrator.

Adding an Existing User as a Cloud Provider Technical Administrator

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 Cloud Portal 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 Cloud Portal will be overwritten by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

Assign an existing user the Cloud Provider Technical Administrator role.

When you assign the Cloud Provider Technical Administrator role, the user's organization unit automatically changes to the Cloud Provider Technical Administrator organization, and the user's current organization is removed.

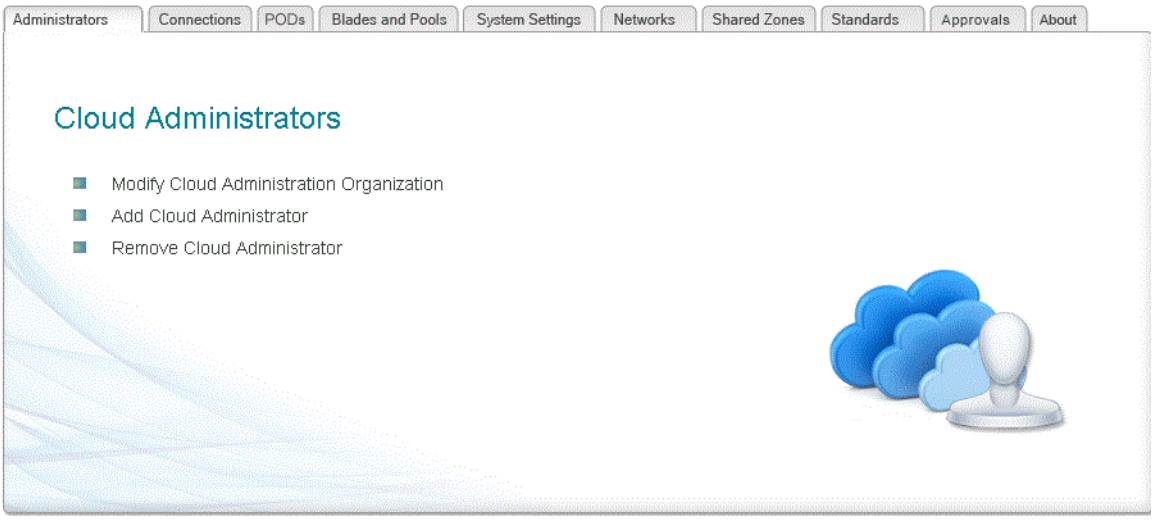
For example, a user belongs to an organization called "HR." If the user is added as a Cloud Provider Technical Administrator, the user's organization becomes the Cloud Provider Technical Administrator organization, and the user's membership in the HR organization is removed.

Note For information on the Cloud Provider Technical Administrator role, see Cloud Provider Technical Administrator, page 1-17.

Step 1 Choose **My Workspace** from the module drop-down list, then click the **System Setup** tab to open the portal.

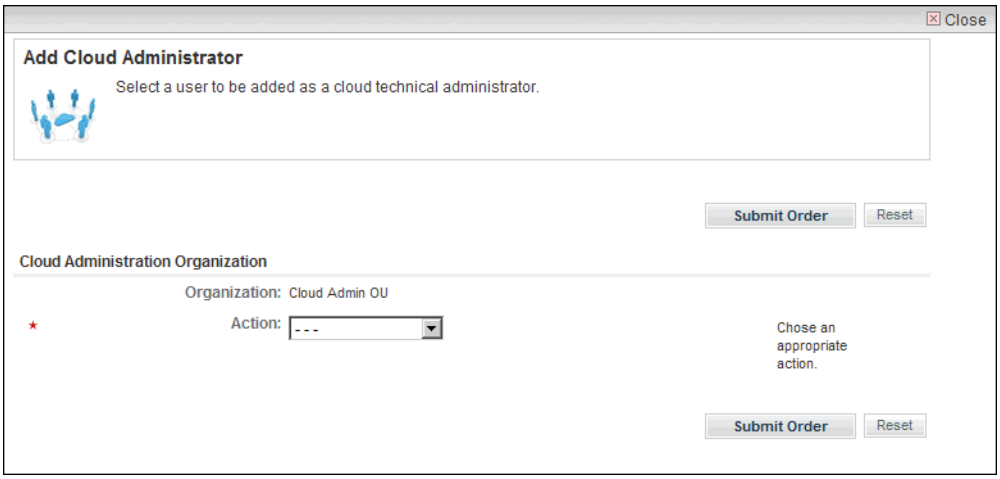
The Cloud Administrators portlet is displayed by default.

Figure 4-6 Cloud Administrators Portlet



Step 2 On the Cloud Administrators portlet, click **Add Cloud Administrator** to open the form.

Figure 4-7 Add Cloud Administrator Form

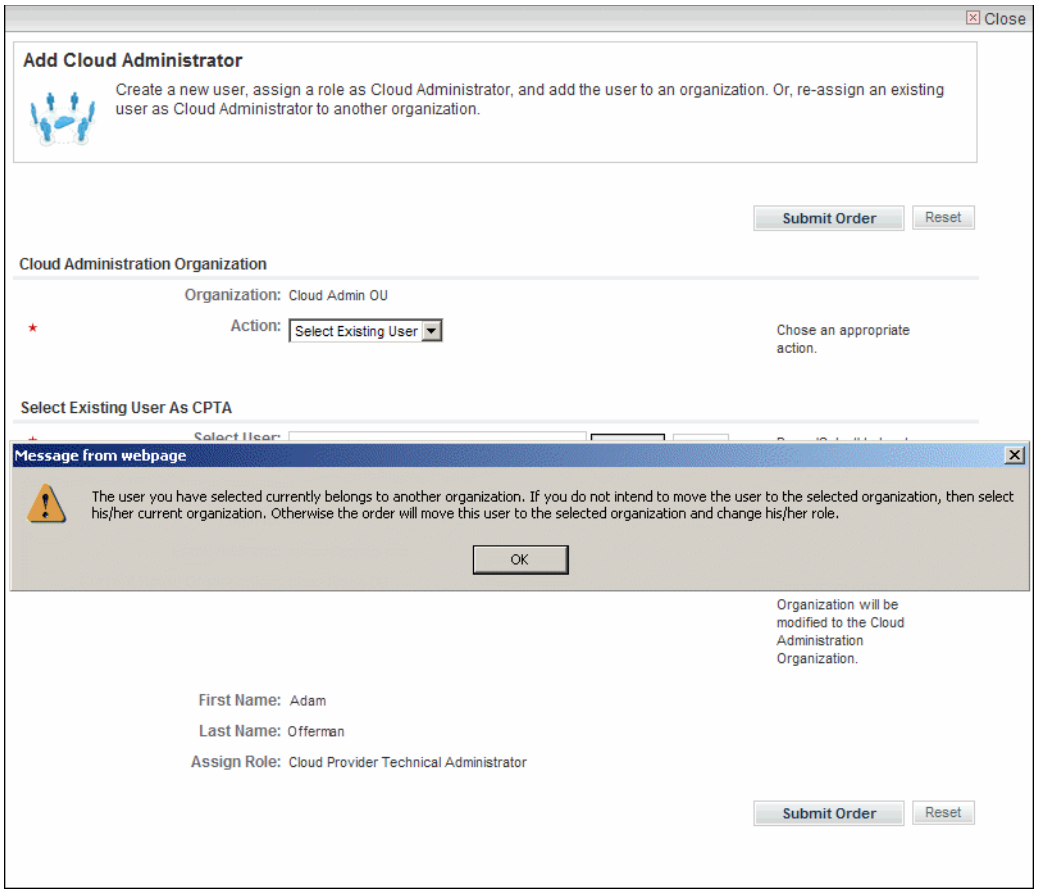


Note If the information shown in Figure 4-1 appears on the form, then directory integration is enabled for your environment. In this case, see Managing Organizations and Users With Directory Integration, page 4-2 before proceeding.

Step 3 On the Add Cloud Administrator form, choose **Select Existing User** from the Action drop-down list.

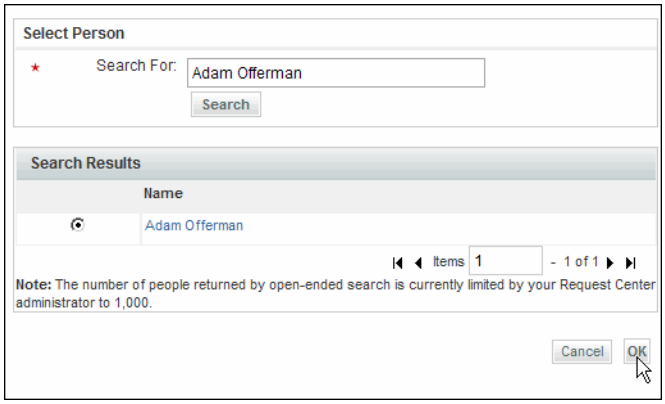
An alert (Figure 4-8 on page 4-9) appears, advising you that the user's organization will change to that of the Cloud Technical Provider Administrator organization. If you are sure you want to proceed, click **OK**.

Figure 4-8 Add Cloud Administrator Form—Select Existing User



Step 4 In the Select User field, click **Select** to open the Select Person dialog box.

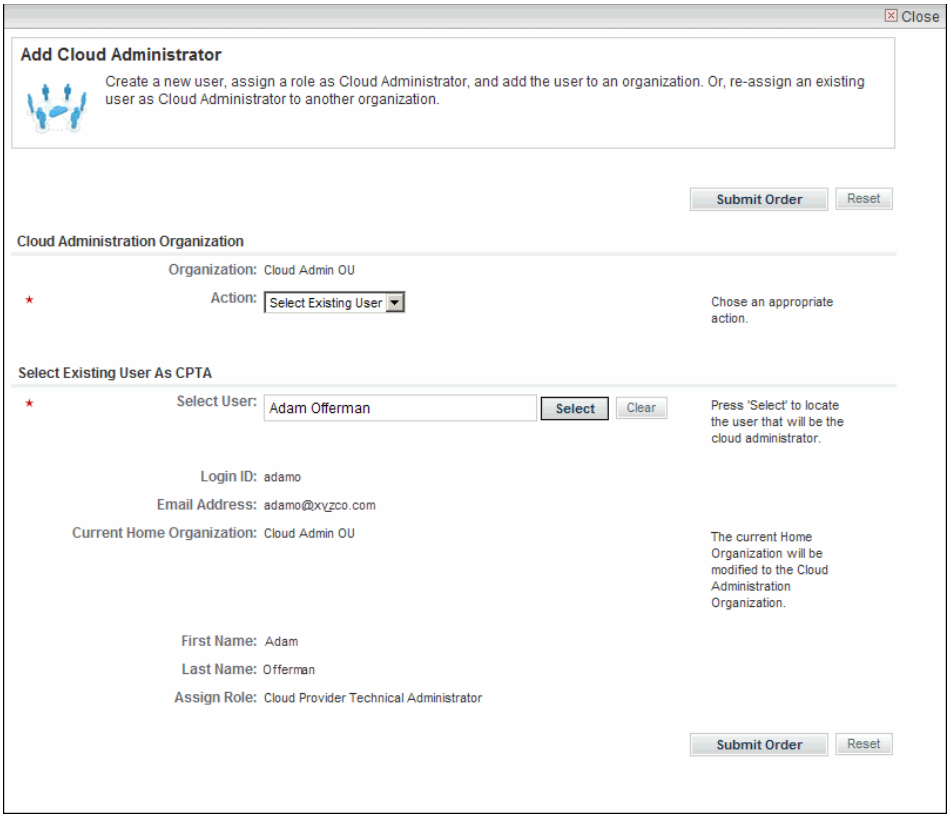
Figure 4-9 Select Person Dialog Box



Step 5 Enter the First Name or Last Name of the user, or enter a wildcard *, and click **Search** to find the user.

Step 6 In the Search Results area, click the radio button next to the name of the user, then click **OK**.

Figure 4-10 Add Cloud Administrator Form—Select Existing User



Step 7 Click **Submit Order**.

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

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 Cloud Portal 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 Cloud Portal will be overwritten by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

Create a new user to add a Cloud Provider Technical Administrator.

Note For information on the Cloud Provider Technical Administrator role, see Cloud Provider Technical Administrator, page 1-17.

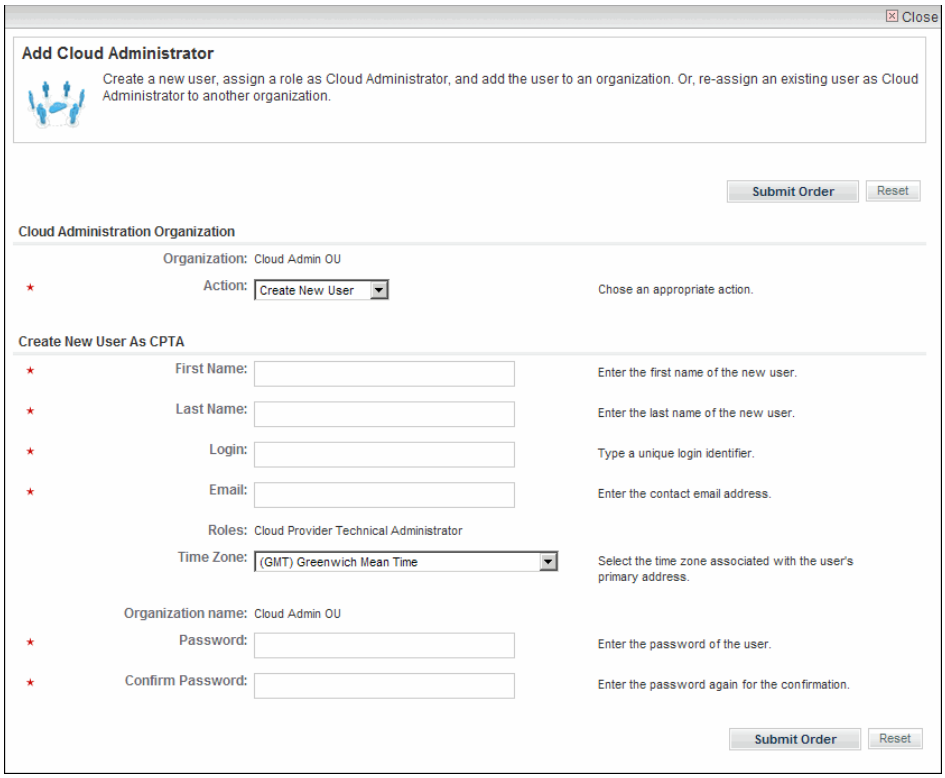
Step 1 Choose **My Workspace** from the module drop-down list, then click the **System Setup** tab to open the portal.

The Cloud Administrators portlet (Figure 4-6 on page 4-7) is displayed.

Step 2 On the Cloud Administrators portlet, click **Add Cloud Administrator** to open the form (Figure 4-7 on page 4-8).

Step 3 On the Add Cloud Administrator form, choose **Create New User** from the Action drop-down list.

Figure 4-11 Add Cloud Administrator Form—Create New User



Step 4 Provide the following information:

Field	Action
First Name Last Name	Enter the first and last name of the new Cloud Provider Technical Administrator.
Login	Enter a unique login identifier for the Cloud Provider Technical Administrator.
Email	Enter the new Cloud Provider Technical Administrator's email address.
Time Zone	From the drop-down list, choose the time zone associated with the new Cloud Provider Technical Administrator's primary address.
Password Confirm Password	Enter and then re-enter the password for the new Cloud Provider Technical Administrator.

Step 5 Click **Submit Order**.

Removing a Cloud Provider Technical Administrator

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 Cloud Portal 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 Cloud Portal will be overwritten by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

Remove the Cloud Portal Technical Administrator role from a user without deleting the user.

Note When a user's role is removed, the user's account status is automatically changed to Inactive, and the user becomes "roleless". Inactive users can log in to Cloud Portal but cannot use any of its services. If you assign the user another role, you must change the user's status back to Active.

If you the a user another role, you must also status from inactive. See Changing a User's Status to Active or Inactive, page 4-27.

Note For information on the Cloud Provider Technical Administrator role, see Cloud Provider Technical Administrator, page 1-17.

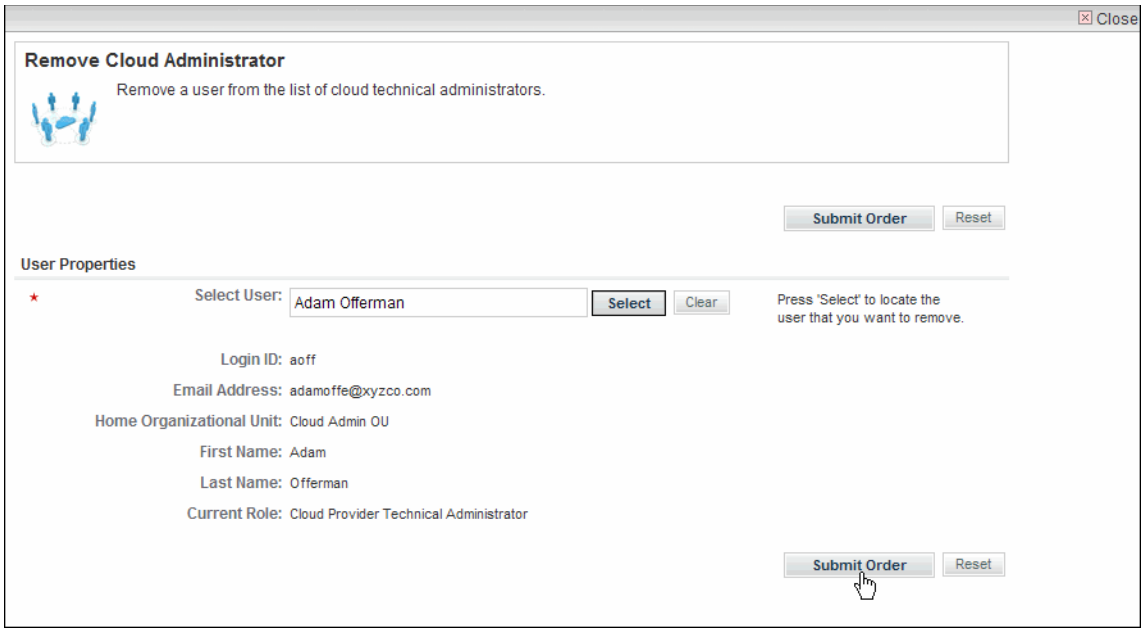
Step 1 Choose **My Workspace** from the module drop-down list, then click the **System Setup** tab to open the portal.

The Cloud Administrators portlet (Figure 4-6 on page 4-7) is displayed.

Step 2 On the Cloud Administrators portlet, click **Remove Cloud Administrator** to open the form.

Note If the information shown in Figure 4-1 appears on the form, then directory integration is enabled for your environment. In this case, see Managing Organizations and Users With Directory Integration, page 4-2 before proceeding.

Figure 4-12 Remove Cloud Administrator Form



Step 3 On the Remove Cloud Administrator form, click **Select** to open the Select Person dialog box (Figure 4-9 on page 4-9).

Step 4 Enter the First Name or Last Name of the user, or enter a wildcard *, and click **Search**.

Step 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.

Step 6 Click **Submit Order**.

Adding or Removing an Organization Technical Administrator

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 Cloud Portal 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 Cloud Portal will be overwritten by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

Change an existing user's role to Organization Technical Administrator for an organization, or remove the user's Organization Technical Administrator role without deleting the user.

The following sections provider instructions for managing users in the Organization Technical Administrator role.

- Creating a New User to Add as an Organization Technical Administrator, page 4-16—Assign the Organization Technical Administrator role to a user who has already been created in the Cloud system.
- Creating a New User to Add as an Organization Technical Administrator, page 4-16—Create a new user, then add the assign the Organization Technical Administrator role to the new user.
- Removing an Organizational Technical Administrator, page 4-18—Remove an Organization Technical Administrator.

Adding an Existing User as an Organization Technical Administrator

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 Cloud Portal 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 Cloud Portal will be overwritten by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

Add an existing user as an Organization Technical Administrator.

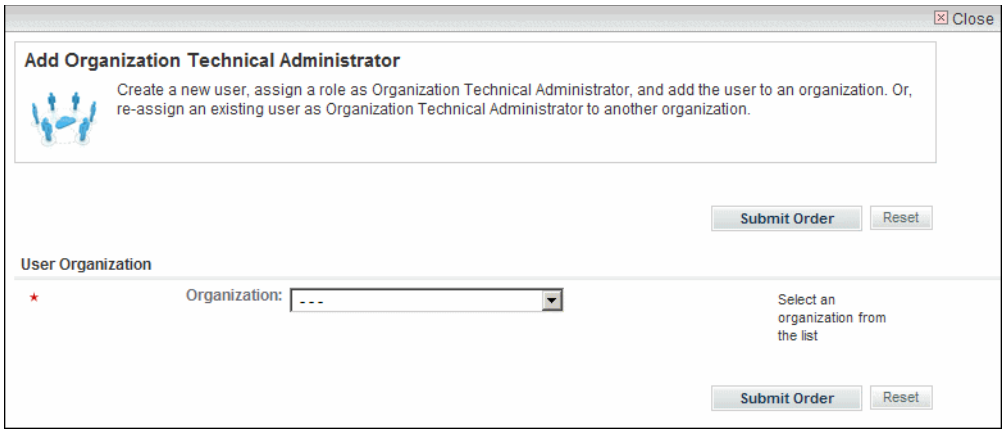
Note For information on the Organization Technical Administrator role, see Organization Technical Administrator, page 1-18.

Step 1 Choose **My Workspace** from the module drop-down list, then click the **Organization Management** tab.

Step 2 On the Organization Management portal (Figure 4-2 on page 4-3), click **Add Organization Technical Administrator** to open the form.

Note If the information shown in Figure 4-1 appears on the form, then directory integration is enabled for your environment. In this case, see Managing Organizations and Users With Directory Integration, page 4-2 before proceeding.

Figure 4-13 Add Organization Technical Administrator Form



Step 3 On the Add Organization Technical Administrator form, choose the organization to which you want to assign the user from the drop-down list.

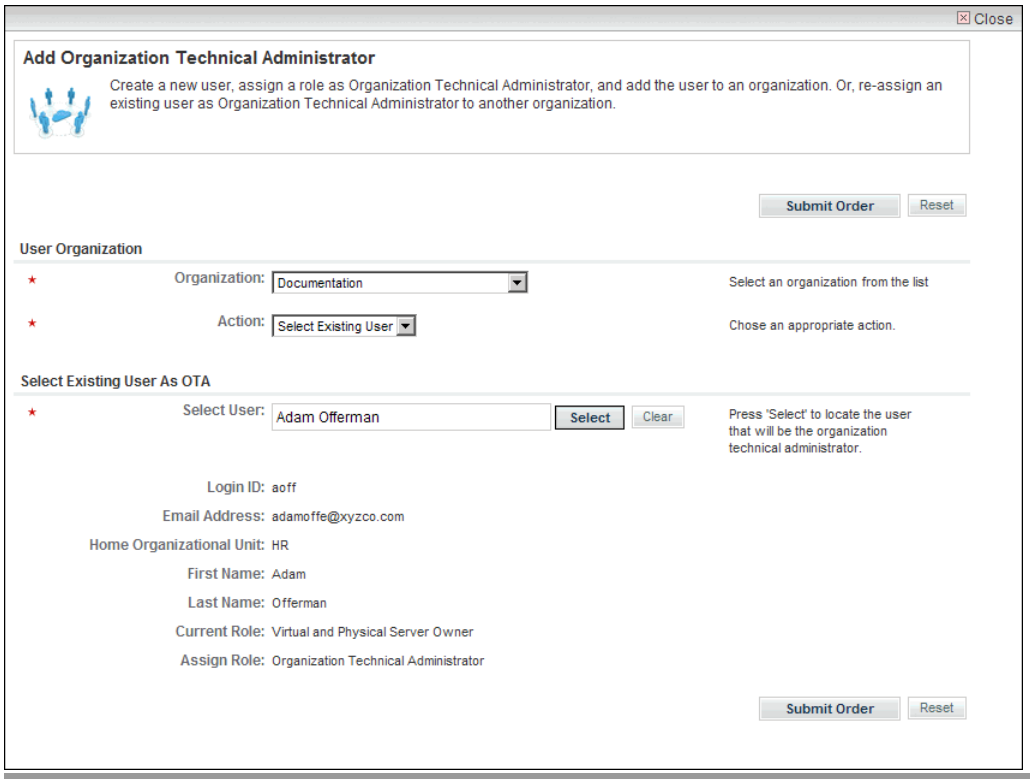
Step 4 In the User Properties area, click **Select** to open the Select Person dialog box (Figure 4-9 on page 4-9).

Step 5 Enter the First Name or Last Name of the user, or enter a wildcard *, and click **Search** to find the user.

Step 6 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**.

Step 7 Click **Submit Order**.

Figure 4-14 Add Organization Technical Administrator Form—Select Existing User



Creating a New User to Add as an Organization Technical Administrator

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 Cloud Portal 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 Cloud Portal will be overwritten by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

Create a new user to add a Cloud Provider Technical Administrator.

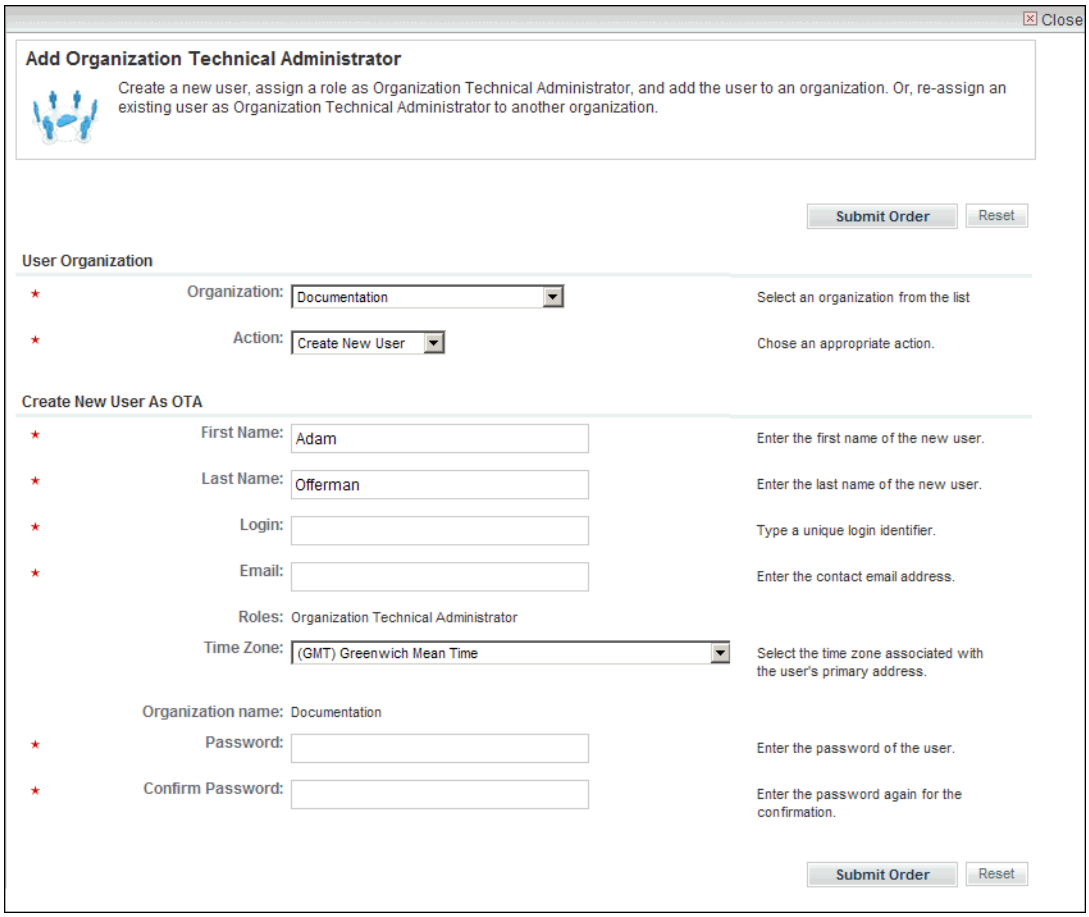
Note For information on the Organization Technical Administrator role, see Organization Technical Administrator, page 1-18.

Step 1 Choose **My Workspace** from the module drop-down list, then click the **Organization Management** tab to open the portal.

Step 2 On the Organization Management portal, click **Add Organization Technical Administrator** to open the form.

Step 3 On the Add Cloud Administrator form (Figure 4-13 on page 4-15), choose **Create New User** from the Action drop-down list.

Figure 4-15 Add Organization Technical Administrator Form—Create New User



Step 4 Provide the following information:

Field	Action
First Name Last Name	Enter the first and last name of the new Organization Technical Administrator.
Login	Enter a unique login identifier for the new Organization Technical Administrator.
Email	Enter the new Organization Technical Administrator's email address.
Time Zone	From the drop-down list, choose the time zone associated with the new Organization Technical Administrator's primary address.
Password Confirm Password	Enter and then re-enter the password for the new Organization Technical Administrator.

Step 5 Click **Submit Order**.

Removing an Organizational Technical Administrator

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 Cloud Portal 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 Cloud Portal will be overwritten by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

Remove the Organization Technical Administrator from a user without deleting the user.

Note When a user's role is removed, the user becomes "roleless" and Status is automatically changed to Inactive. Inactive users can log in to Cloud Portal but cannot use any of its services. If you assign the user another role, you must change the user's status back to Active.

If you the a user another role, you must also status from inactive. See Changing a User's Status to Active or Inactive, page 4-27.

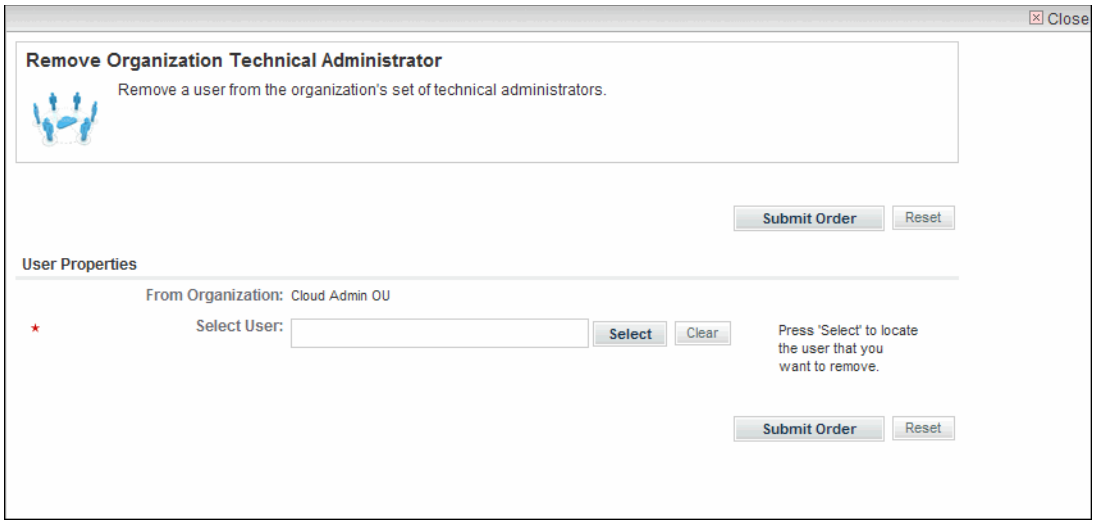
Note For information on the Organization Technical Administrator role, see Organization Technical Administrator, page 1-18.

Step 1 Choose **My Workspace** from the module drop-down list, then click the **Organization Management** tab.

Step 2 On the Organization Management portal (Figure 4-2 on page 4-3), click **Remove Organization Technical Administrator** to open the form.

Note If the information shown in Figure 4-1 appears on the form, then directory integration is enabled for your environment. In this case, see Managing Organizations and Users With Directory Integration, page 4-2 before proceeding.

Figure 4-16 Remove Organization Technical Administrator Form



Step 3 On the Remove Organization Technical Administrator form, click **Select** to open the Select Person dialog box (Figure 4-9 on page 4-9).

Step 4 Enter the First Name or Last Name of the user, or enter a wildcard *, and click **Search** to find the user.

Step 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.

Step 6 Click **Submit Order**.

Adding or Removing a Server Owner

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 Cloud Portal 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 Cloud Portal will be overwritten by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

Assign a Virtual Server Owner or Virtual and Physical Server Owner role to a new or existing user.

Note For more information about the Server Owner roles, see Virtual Server Owner, page 1-18 and Virtual and Physical Server Owner, page 1-18.

Use one of the two following procedures to add a Server Owner. The method you choose depends on whether you are using a directory service to import, authenticate, authorize users.

- Adding an Existing User as a Server Owner, page 4-20—Add an existing user an as a Virtual Server Owner or Virtual and Physical Server Owner within an organization.
- Creating a New User to Add as a Server Owner, page 4-22—Create a new user and then add the new user as an Virtual Server Owner or Virtual and Physical Server Owner within an organization.
- Removing a Server Owner, page 4-23—Remove a Virtual Server Owner or Virtual and Physical Server Owner.
- If you are unsure whether directory integration is enabled in your Cloud environment, the information shown in Figure 4-1 on page 4-2 will appear on the Add User form. In that case, see the following section, Adding an Existing User as a Server Owner.

Adding an Existing User as a Server Owner

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 Cloud Portal 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 Cloud Portal will be overwritten by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

Note For information on the Server Owner roles, see Virtual Server Owner, page 1-18 and Virtual and Physical Server Owner, page 1-18.

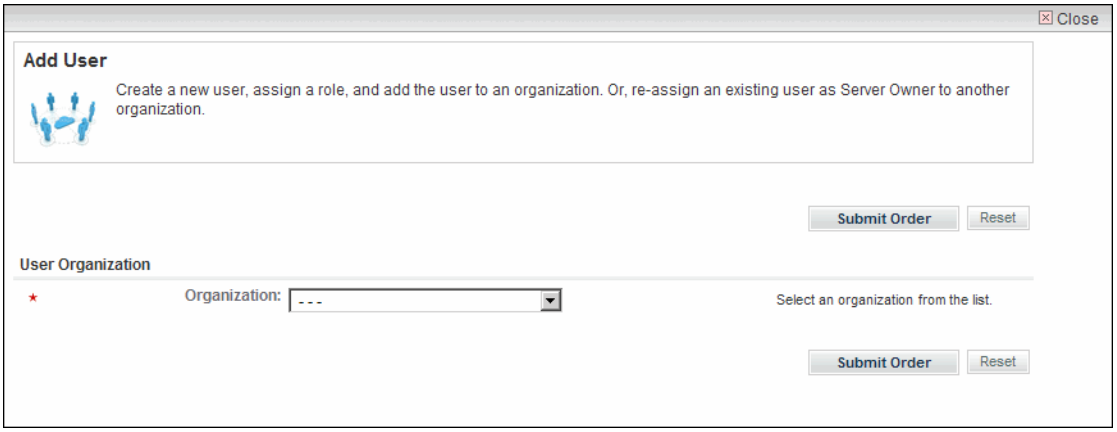
Step 1 Choose **My Workspace** from the module drop-down list, then click the **User Management** tab to open the portal page.

Figure 4-17 User Management Portal

Step 2 On the User Management portal page, click **Add User** to open the form.

Note If the information shown in Figure 4-1 appears on the form, then directory integration is enabled for your environment. In this case, see Managing Organizations and Users With Directory Integration, page 4-2, before proceeding.

Figure 4-18 Add User Form



Step 3 On the Add User form, choose the organization to which you want to add the user from the Organization drop-down list.

Step 4 Choose **Select Existing User** from the Action drop-down list to display the Select 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 selected. If this is acceptable, click **OK**.

Step 5 Click **Select** to open the Select Person dialog box (Figure 4-9 on page 4-9).

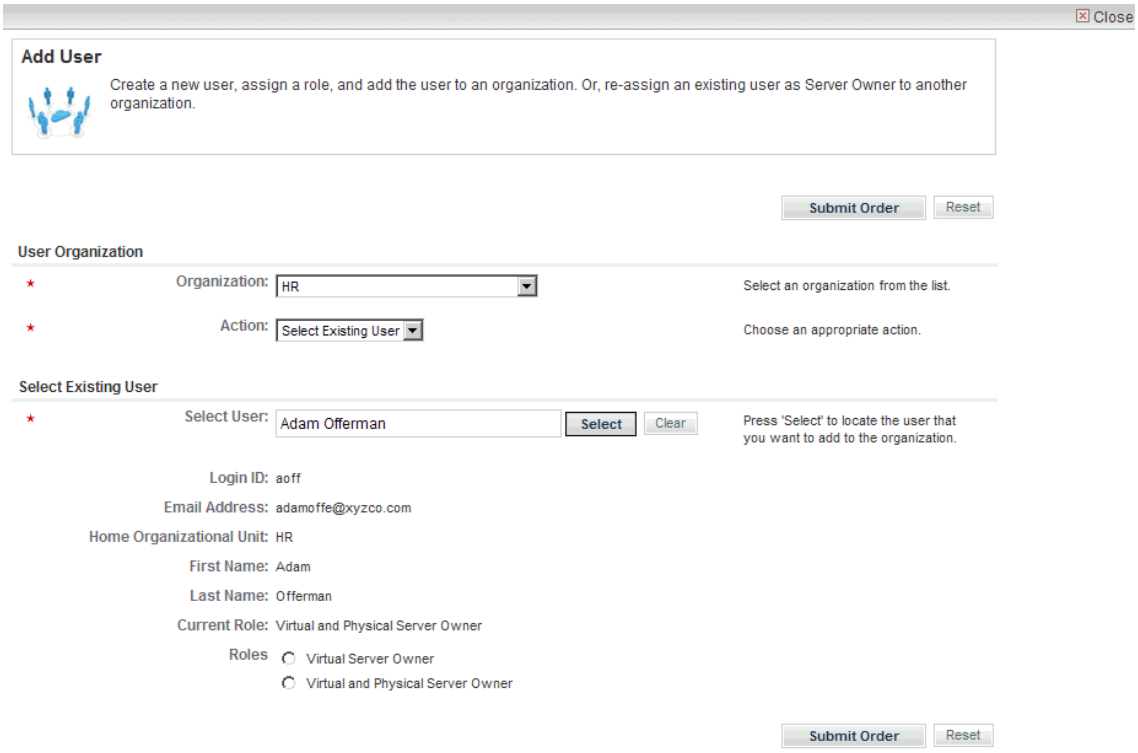
Step 6 In the Select User field, click **Select** to open the Select Person dialog box.

Step 7 Enter the First Name or Last Name of the user, or enter a wildcard *, and click **Search**.

Step 8 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.

Figure 4-19 Add User Form—Add Existing User



Step 9 Click **Submit Order**.

Creating a New User to Add as a Server Owner

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 Cloud Portal 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 Cloud Portal will be overwritten by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

Create a new user to add a Cloud Provider Technical Administrator.

Note For information on the Server Owner roles, see Virtual Server Owner, page 1-18 and Virtual and Physical Server Owner, page 1-18.

Step 1 Choose **My Workspace** from the module drop-down list, then click the **User Management** tab to open the portal page.

Step 2 On the User Manager portal page (Figure 4-17 on page 4-21), click **Add User** to open the form.

Step 3 On the Add User form (Figure 4-18 on page 4-21), choose the organization to which you want to add the user from the Organization drop-down list.

Step 4 Choose **Create New User** from the Action drop-down list.

Step 5 Provide the following information:

Field	Action
First Name Last Name	Enter the first and last name of the new user.
Login	Enter a unique login identifier for the user.
Email	Enter the user's email address.
Time Zone	From the drop-down list, choose the time zone associated with the user's primary address.
Password Confirm Password	Enter and then re-enter the password for the user.

Step 6 Click **Submit Order**.

Removing a Server Owner

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 Cloud Portal 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 Cloud Portal will be overwritten by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

Remove the Virtual or Virtual and Physical Server Owner role from a user, without deleting the user.

Note When a user's role is removed, the user's account status is automatically changed to Inactive, and the user becomes "roleless". Inactive users can log in to Cloud Portal but cannot use any of its services. If you assign the user another role, you must change the user's status back to Active.

If you the a user another role, you must also status from inactive. See Changing a User's Status to Active or Inactive, page 4-27.

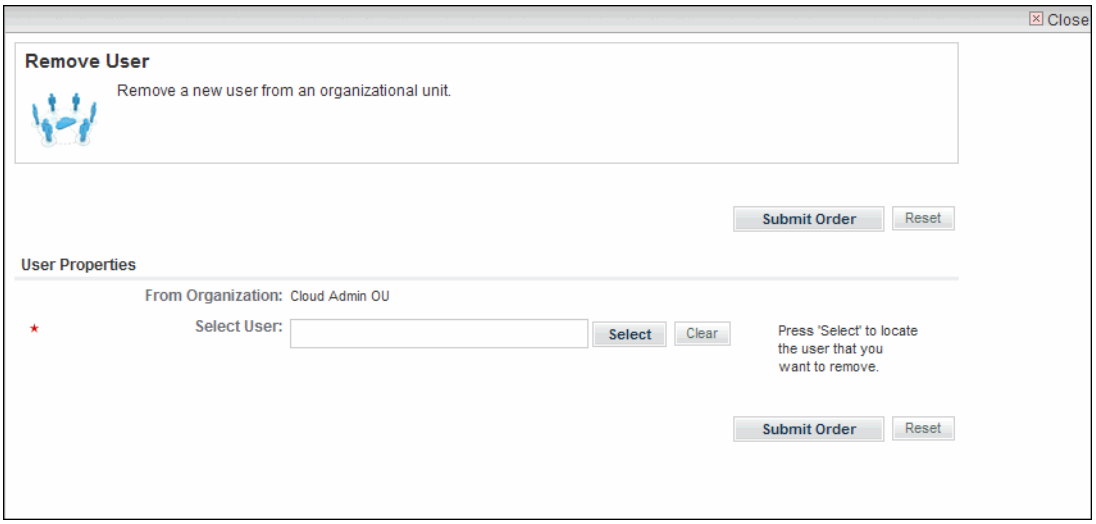
Note For information on the Server Owner roles, see Virtual Server Owner, page 1-18 and Virtual and Physical Server Owner, page 1-18.

Step 1 Choose **My Workspace** from the module drop-down list, then click the **User Management** tab.

Step 2 On the User Management portal (Figure 4-17 on page 4-21), click **Remove User** to open the form.

Note If the information shown in Figure 4-1 appears on the form, then directory integration is enabled for your environment. In this case, see Managing Organizations and Users With Directory Integration, page 4-2 before proceeding.

Figure 4-20 Remove User Form



Step 3 On the Remove User form, click **Select** to open the Select Person dialog box (Figure 4-9 on page 4-9).

Step 4 Enter the First Name or Last Name of the user, or enter a wildcard *, and click **Search** to find the user.

Step 5 In the Search Results area, click the radio button next to the name of the user you want to remove as a Virtual or Virtual and Physical Server Owner, then click **OK**.

Properties for the user display on the form.

Step 6 Click **Submit Order**.

Modifying User Properties

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 Cloud Portal 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 Cloud Portal will be overwritten by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

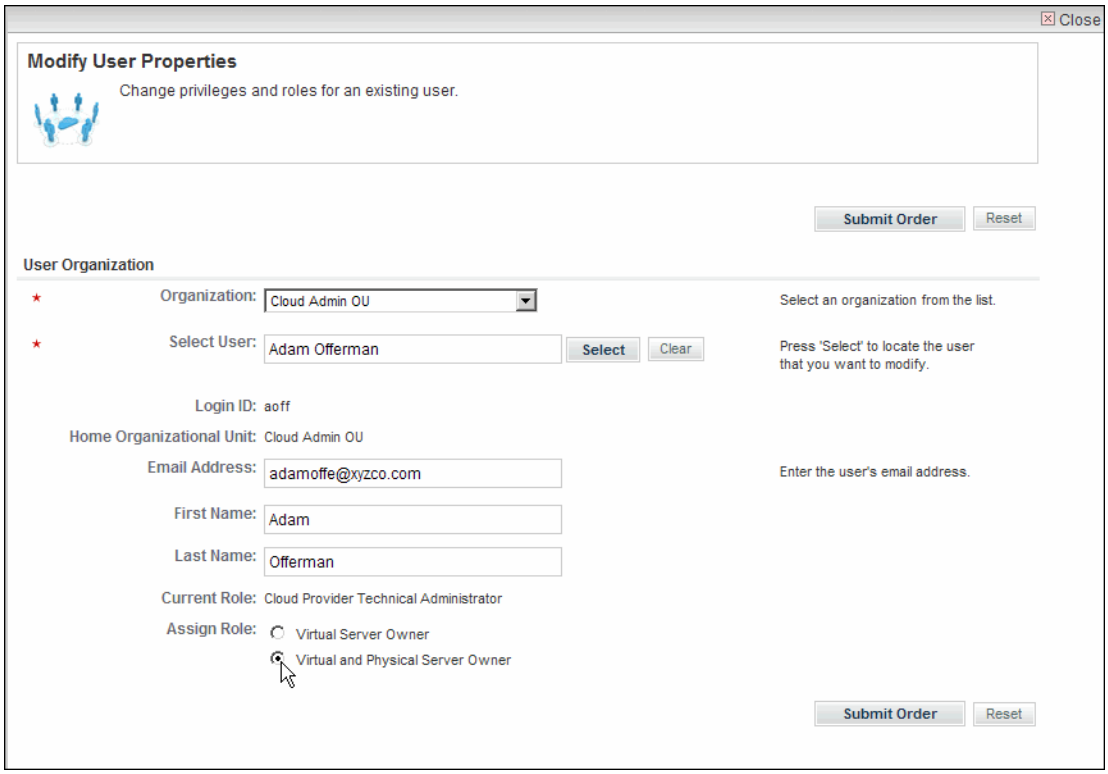
Update a user's first name, last name, or email address, or add or change a Server Owner role.

Note You can also optionally add or modify calendar and additional contact information from the Organization Designer module. For information, see Figure 4-21 on page 4-26.

Step 1 Choose **My Workspace** from the module drop-down list and click the **User Management** tab.

Step 2 On the User Management portal (Figure 4-17 on page 4-21), click **Modify User Properties** to open the form.

Figure 4-21 Modify User Properties Form



Step 3 On the Modify User Properties form, choose the user's organization from the **Organization** drop-down menu.

Step 4 In the Select User field, click **Select** to open the Select Person dialog box (Figure 4-9 on page 4-9).

The user's current home organization and role appear.

Step 5 *Optional*. Update the user's first name, last name, or email address.

Step 6 *Optional*. Add a Server Owner role, or change the user's existing Server Owner role by clicking the **Virtual Server Owner** or **Virtual and Physical Server Owner** radio button.

Step 7 Click **Submit Order**.

Adding or Modifying User Details

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 Cloud Portal 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 Cloud Portal will be overwritten by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

In the Organization Designer module, you can add, update, or delete optional details about a user, such as additional contact and calendar information.

Although such details are optional in Cloud Portal, they may be useful or required by the user's organization.

If you modify a user's name or email address, the change appears globally in Cloud Portal.

Note You can also modify a user's name and email address from the User Management portal. You can also use the form to assign the user a Server Owner role. The changes appear globally. For information, see Figure 4-20 on page 4-25.

Note If external authentication is enabled for your environment, you must modify user details from the directory. See Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

Step 1 Choose **Organization Designer** from the module drop-down list and click the **People** tab.

Step 2 On the Organization Designer Home page (Figure 1-6 on page 1-7), 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.

Step 3 Use the menu on the right to make any or all of the updates:

- General—First and last name, time zone, and login information
- Address—Company and personal mailing addresses
- Contact—Business and personal email addresses, phone numbers, and fax numbers
- Extensions—Information about the user within the business structure, such as cost center number, employee type, and management level. Includes customizable fields.
- Calendar—Schedule of the user's typical hours of availability and non-working days, and special dates.

Changing a User's Status to Active or Inactive

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 Cloud Portal 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 Cloud Portal will be overwritten by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

When users are created in Cloud Portal or imported to Cloud Portal 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 Cloud Portal 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. 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.

To change a user's status to Active or Inactive, perform the following steps.

Step 1 Choose **Organization Designer** from the module drop-down list and click the **People** tab.

Step 2 On the Organization Designer Home page (Figure 1-6 on page 1-7), 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.

Note The names of users with inactive status appear in the People list in italics with strike-through.

Step 3 In the General pane, choose **Active** or **Inactive** from the Status drop-down menu.

Step 4 Click **Update**.

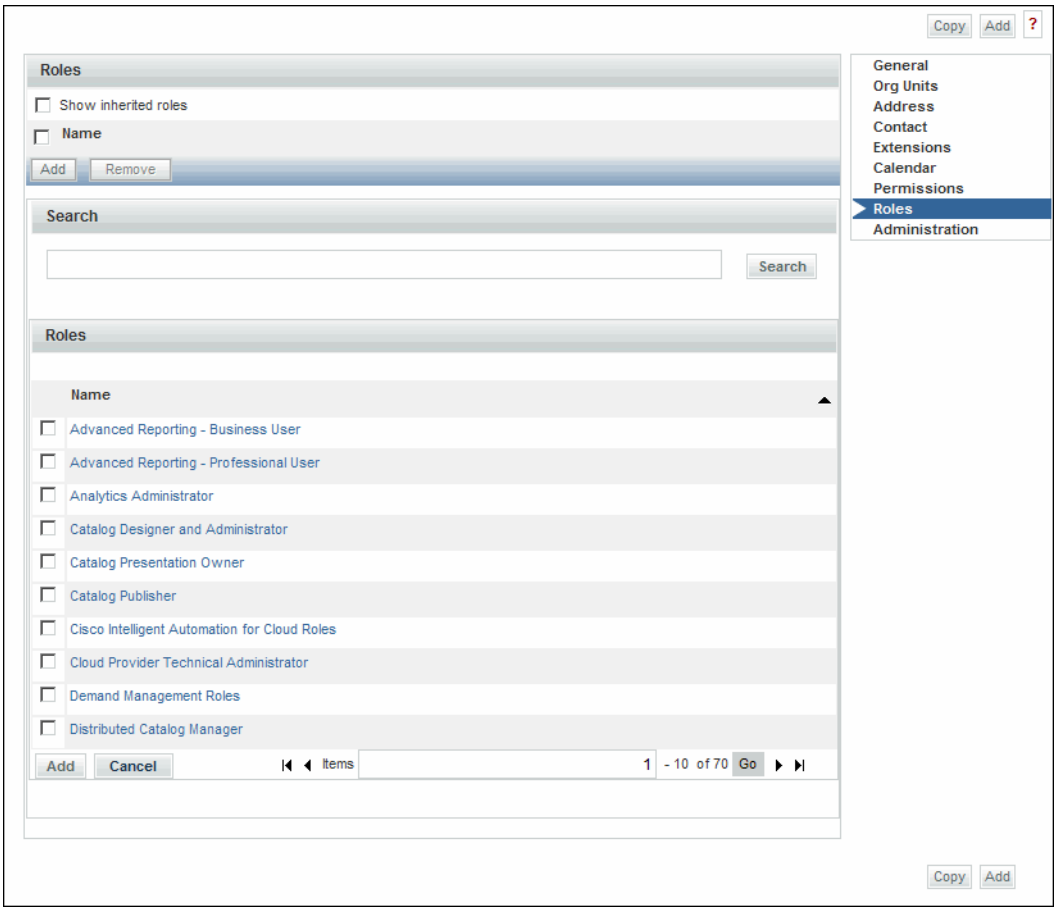
Note If you are changing the user's status to Active, you may need to assign a role. If you are unsure of the user's role, do not navigate away from the user details page, and see the following steps.

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 Cloud Portal.

Step 1 On the user's details page, click **Roles** in the menu on the right.

Step 2 In the Roles pane, click **Add** to expand the Roles list.

Figure 4-22 Organization Designer—Roles List



Step 3 In the Roles list, locate the role that you want to assign to the user, check the check box, then click **Add**.

Managing User Roles

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 Cloud Portal 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 Cloud Portal will be overwritten by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

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.

Assigning a User to a Server Owner Role

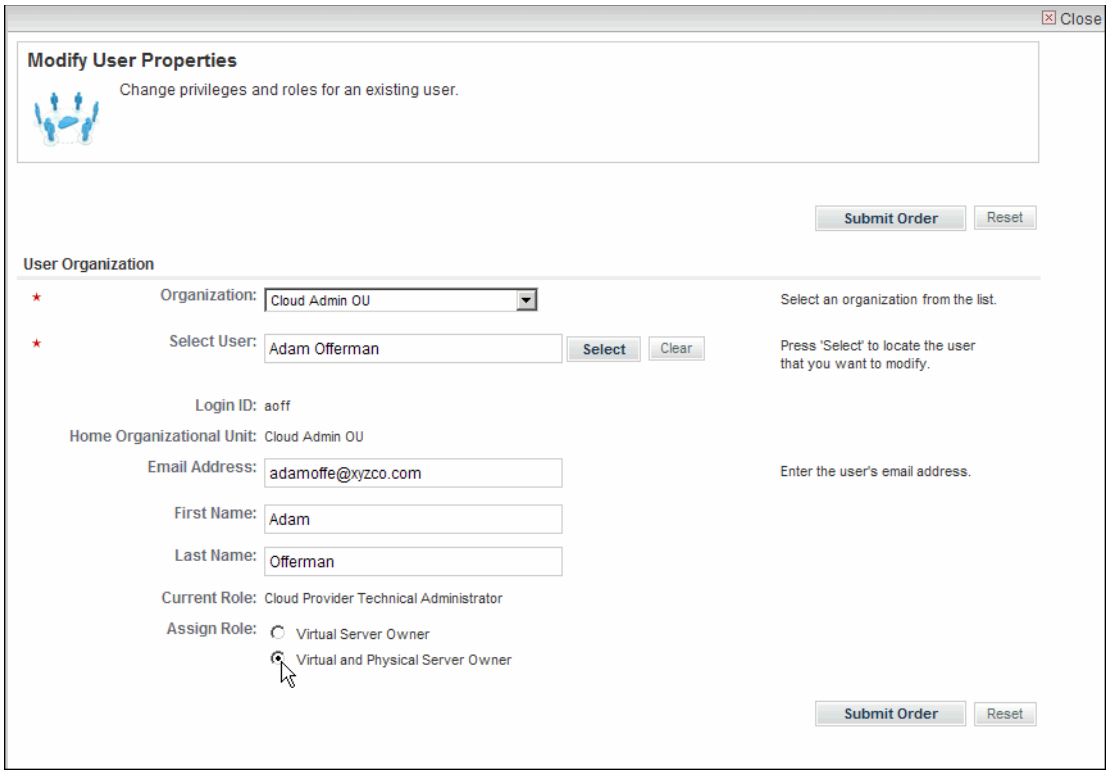
Note If directory authorization has been enabled for your Cloud environment, then you may have to create users and assign, change, or remove roles from the directory rather than by using the Cloud Portal services outlined in this section. Directory integration can be configured so that users must be managed from the directory. In this case, any changes you make to an user using Cloud Portal will be overwritten by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

Note For information on the Server Owner roles, see Virtual Server Owner, page 1-18 and Virtual and Physical Server Owner, page 1-18.

Step 1 Choose **My Workspace** from the module drop-down list and click the **User Management** tab.

Step 2 On the User Management portal (Figure 4-17 on page 4-21), click **Modify User Properties** to open the form.

Figure 4-23 Modify User Properties Form



Step 3 On the Modify User Properties form, choose the user's organization from the **Organization** drop-down menu.

Step 4 In the Select User field, click **Select** to open the Select Person dialog box (Figure 4-9 on page 4-9).

The user's current home organization and role appear.

Step 5 *Optional*. Update the user's email address, first name, and last name.

Step 6 *Optional*. Click either the **Virtual Server Owner** or **Virtual and Physical Server Owner** radio button to assign the user to a Server Owner role, or to change the user's role from one Server Owner role to the other.

Step 7 Click **Submit**.

Reassigning a Server Owner to Another Server Owner Role

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 Cloud Portal 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 Cloud Portal will be overwritten by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

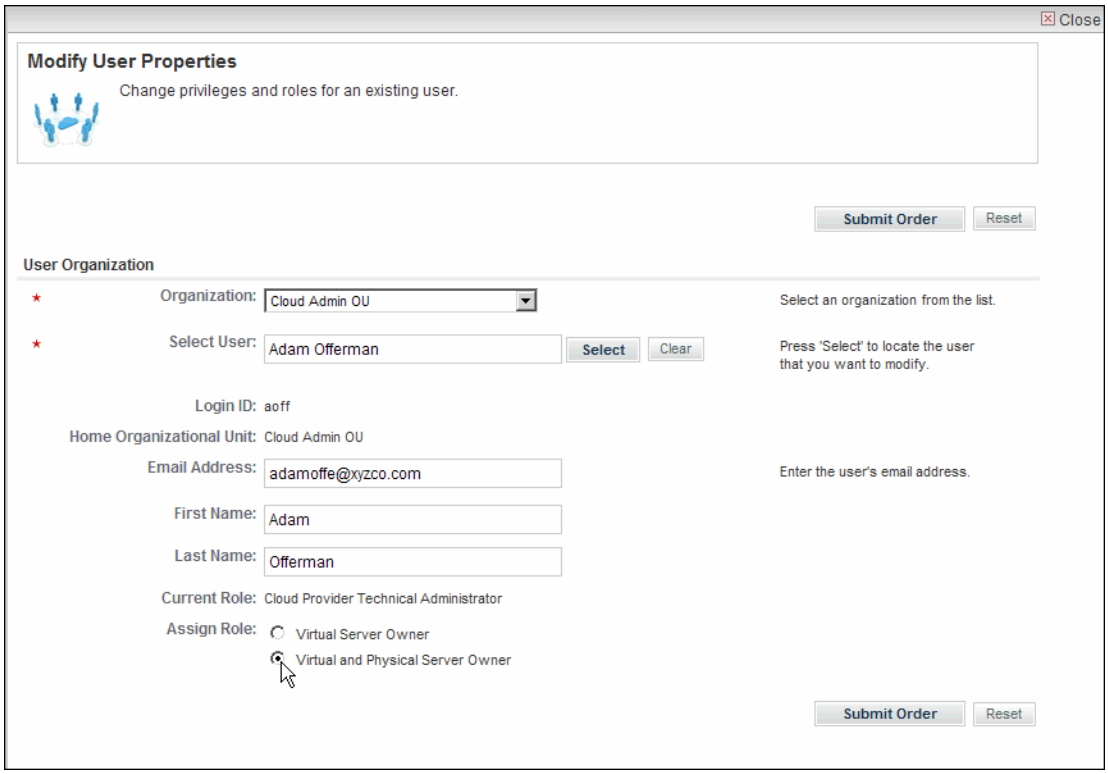
Change a user's Virtual Server Owner role to the Virtual and Physical Server Owner role, or vice versa.

Note For information on the Server Owner roles, see Virtual Server Owner, page 1-18 and Virtual and Physical Server Owner, page 1-18.

Step 1 Choose **My Workspace** from the module drop-down list and click the **User Management** tab.

Step 2 On the User Management portal (Figure 4-17 on page 4-21), click **Modify User Properties** to open the form.

Figure 4-24 Modify User Properties Form



Step 3 On the Modify User Properties form, choose the user's organization from the **Organization** drop-down menu.

Step 4 In the Select User field, click **Select** to open the Select Person dialog box (Figure 4-9 on page 4-9).

The user's current home organization and role appear.

Step 5 *Optional*. Update the user's first name, last name, or email address.

Step 6 For Assigned Role, change the user's Server Owner role by clicking the **Virtual Server Owner** or **Virtual and Physical Server Owner** radio button.

Step 7 Click **Submit Order**.

Reassigning an Organization Technical Administrator as a Server Owner

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 Cloud Portal 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 Cloud Portal will be overwritten by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

Change a user's role within an organization from Organization Technical Administrator to Virtual Server Owner or Virtual and Physical Server Owner.

Note For information on the Server Owner roles, see Virtual Server Owner, page 1-18 and Virtual and Physical Server Owner, page 1-18.

Step 1 Follow the steps for removing an organization technical administrator, outlined in Removing an Organizational Technical Administrator, page 4-18.

Note When a user's role is removed, the user becomes "roleless," and automatically given Inactive status. You must change the user's status back to Active.

Step 2 After submitting the order to remove the role, click **General** in the menu on the right.

Step 3 From the Status drop-down menu, choose **Active**.

Step 4 Click **Update**.

Step 5 Follow the steps for adding a server owner, outlined in Assigning a User to a Server Owner Role, page 4-29.

Reassigning a Server Owner as a Organization Technical Administrator

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 Cloud Portal 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 Cloud Portal will be overwritten by the definitions set in the directory. For more information, see Adding or Removing a Cloud Provider Technical Administrator, page 4-6.

Change a user's role within an organization from Virtual Server Owner or Virtual and Physical Server Owner to Organization Technical Administrator.

Note For information on the Server Owner roles, see Virtual Server Owner, page 1-18 and Virtual and Physical Server Owner, page 1-18.

Step 1 Follow the steps in Reassigning an Organization Technical Administrator as a Server Owner, page 4-32.

Step 2 Follow the steps in Removing an Organization, page 4-5.

Changing the nsAPI User Account Username and Password

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

Changing the credentials for the nsAPI user involves two steps:

- Changing the nsAPI User Credentials in Cloud Portal
- Updating the Associated Extended Target Properties in Process Orchestrator

Changing the nsAPI User Credentials in Cloud Portal

Note For information on how the nsAPI User was created, *see* the *Cisco Intelligent Automation for Cloud 3.1 Configuration Guide*.

Step 1 Choose **Organization Designer** from the module drop-down list, then click the **People** tab.

Step 2 In the People pane on the left, enter **nsapi** in the search field, then click **Search**.

Step 3 Click the nsAPI username to display user information.

Step 4 Edit the values in either or both the username (Login) and password.

Step 5 Click **Update**.

Updating the Associated Extended Target Properties in Process Orchestrator

When you change the nsAPI username, password, or both, you must also edit associated the extended target properties with the new credentials in Process Orchestrator.

You will edit the following extended target properties:

- Cloud.Configuration.CloudPortal.API.Password
- Cloud.Configuration.CloudPortal.API.User

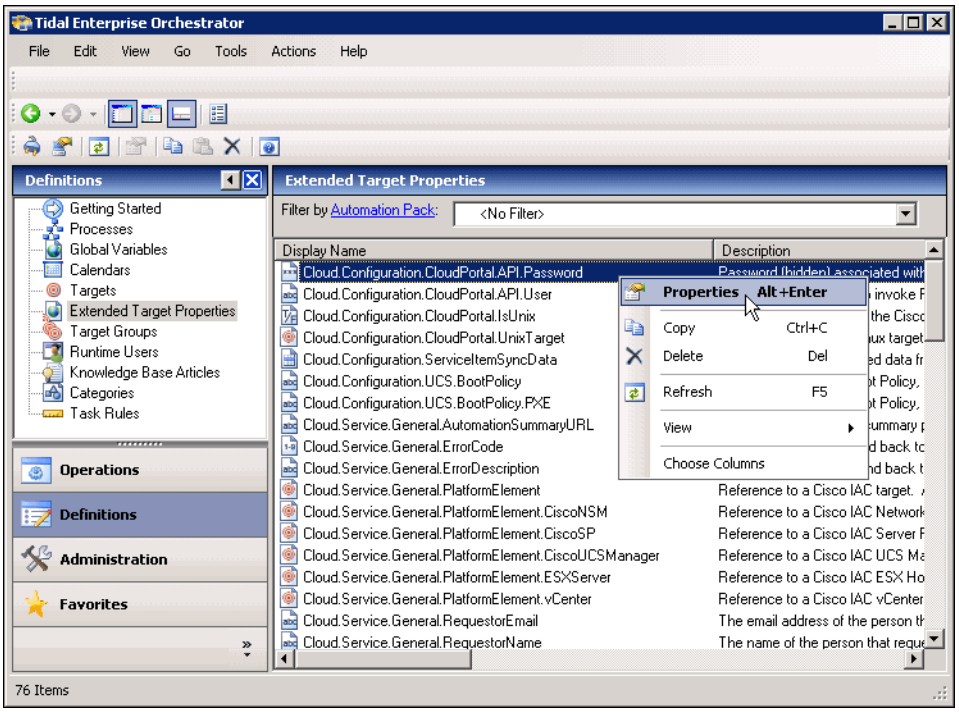
Step 1 Open Process Orchestrator Console and log in.

Step 2 Click Definitions in the navigation pane to display the **Definitions** workspace, if it is not already displaying.

Step 3 In the navigation pane, click **Extended Target Properties**.

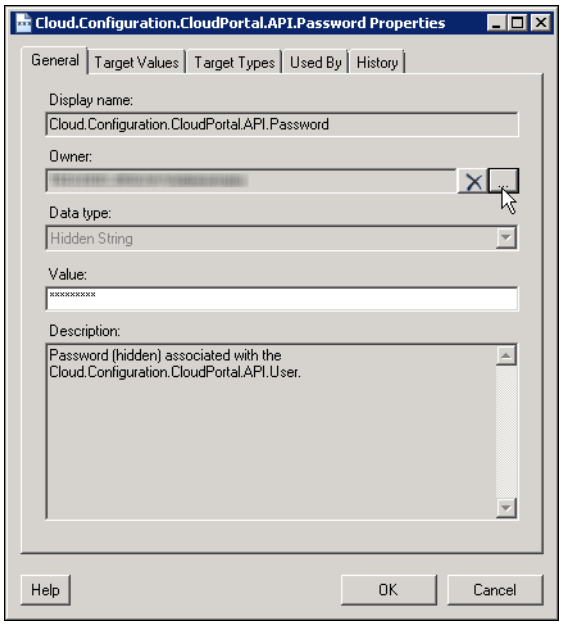
Step 4 In the Extended Target Properties list, right-click Cloud.Configuration.CloudPortal.API.Password and choose **Properties**.

Figure 4-25 Extended Target Property—Opening Properties Dialog Box



Step 5 Right-click Cloud.Configuration.CloudPortal.API.User and choose **Properties**.

Figure 4-26 Extended Target Properties—Properties Dialog Box



Step 6 Click the **Browse** tool beside the Owner field.

Step 7 In the Select User or Group dialog box, enter the username.

Step 8 Click **Check Names** to verify that the user exists.

Note You will be required to log in before the check proceeds.

If the username cannot be verified, double-check the username that you specified in Changing the nsAPI User Credentials in Cloud Portal, page 4-33.

Step 9 Click **OK** to close the Select User or Group dialog box.

Step 10 In Cloud.Configuration.CloudPortal.API.Password dialog box, change the password in the Value field.

Note The password displays as asterisks. Ensure that you enter the password correctly.

Step 11 Click **OK** to complete the procedure.

CHAPTER 5

Managing Services

Cloud Provider Technical Administrators use Cloud Portal to configure standards for service items, manage server leases, and monitor service process flows to ensure they operate smoothly and quickly fix any problems that might arise.

This chapter provides information and steps for managing the service process flow and configuring orderable units. It includes the following sections:

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 **My Workspace**, then click the **Approvals** tab.

Using the Services Manager

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>.

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*.

Step 1 Choose **My Workspace** from the module drop-down list, then click the **My Orders** tab.

Step 2 Select the orders that you want to view. You can choose to view all orders or select based on the status of the service requests. You can also choose to view the requisitions ordered for yourself or for others.

Figure 5-1 Viewing Orders

Step 3 Click + to view the details of the service and the percentage of completion.

Step 4 Click on the order number to view the requisition form that contains the details of the services and the delivery process.

Step 5 Click on the service name to view the order form that contains the service and the server management information.

Step 6 Click **Cancel Service** to cancel the selected service.

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 (see Extending or Removing a Server Lease, page 5-4).
- Storage Lease Expiration—The server is permanently deleted and any stored data is lost.

This section contains the following topics:

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 - Section Warning

You can choose when each email notification is automatically sent. To view and modify the Lease Expiration - First Warning template for the user's organization, see Modifying Email Notification Templates, page 3-55.

Viewing Server Lease Information

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

Step 1 Choose **My Workspace** from the module drop-down list, then click **My Servers**.

Step 2 On the My Servers portal (Figure 3-7 on page 3-12), locate and click the server in the table.

Step 3 Lease information is shown in the Details section for the selected server.

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.

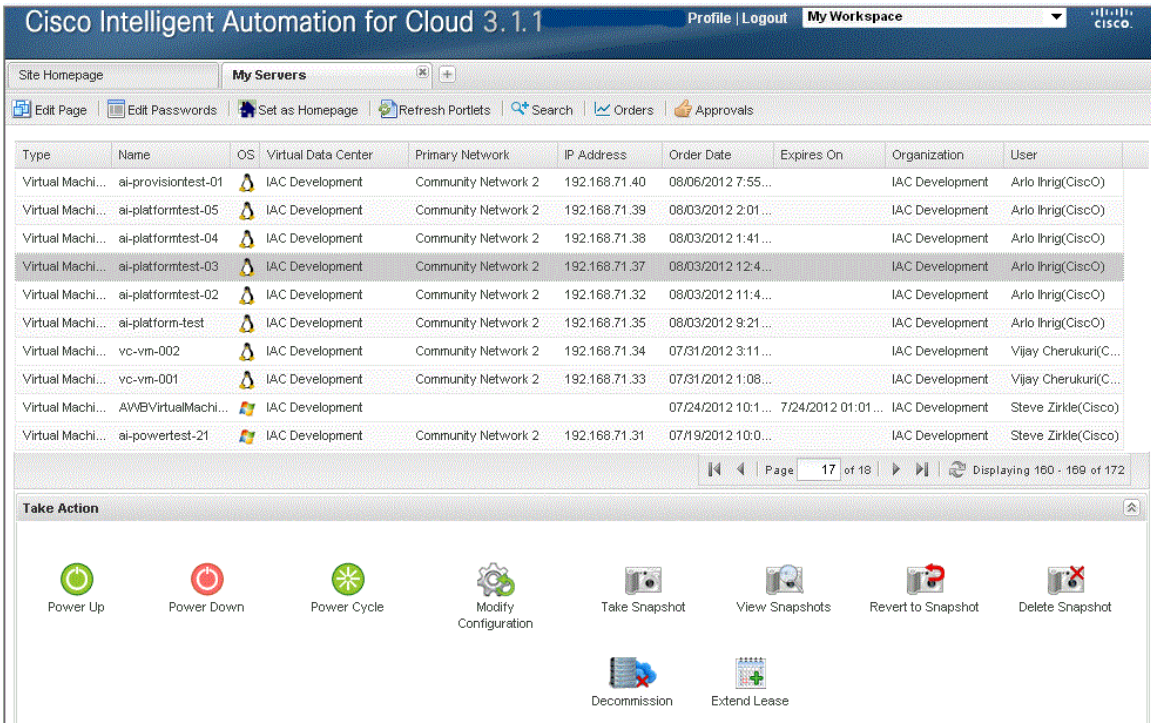
You can also remove an existing lease from a server without deleting or decommissioning it. By removing a lease, you are simply stopping the automatic decommission service.

Step 1 Choose **My Workspace** from the module drop-down list and then click **My Servers**.

Step 2 On the My Servers portal (Figure 3-7 on page 3-12), locate and click the server in the table.

Details about the server and icons for actions appear in the Take Action area.

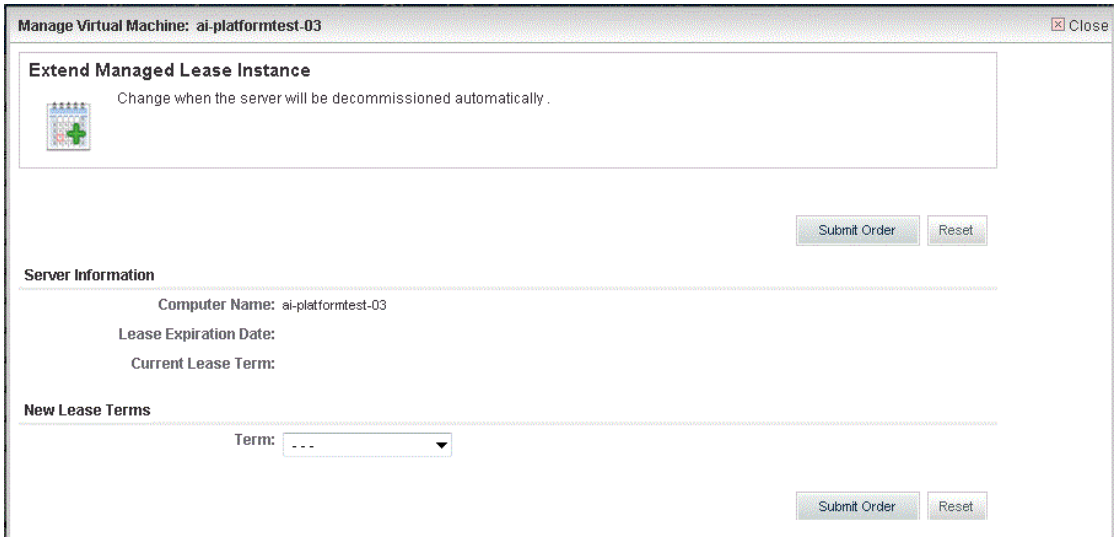
Figure 5-2 Extend Lease



Step 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.

Figure 5-3 Extend Managed Lease Instance Form



Step 4 From the **Term** drop-down list on the Extend Managed Lease Instance form, choose the number of days that you want to add to the end of your lease term, or choose **No Lease** to remove the lease from the server.

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

Step 5 Click **Submit Order**.

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:
  - 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 Cloud Portal
  - Taking manual actions outside the system
  - Restarting the process from Cloud Portal
  - Cancelling 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.

There are three sequential steps involved in remediating an infrastructure error:

- Assigning the Remediation Task for Repair, page 5-6
- Remediating a Service, page 5-8
- Checking the Status of an Order, page 5-10
- Cancelling the Order if Remediation Attempt is Unsuccessful, page 5-11

Assigning the Remediation Task for Repair

Note You must have Cloud Provider Technical Administrator permissions to perform these tasks.

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.

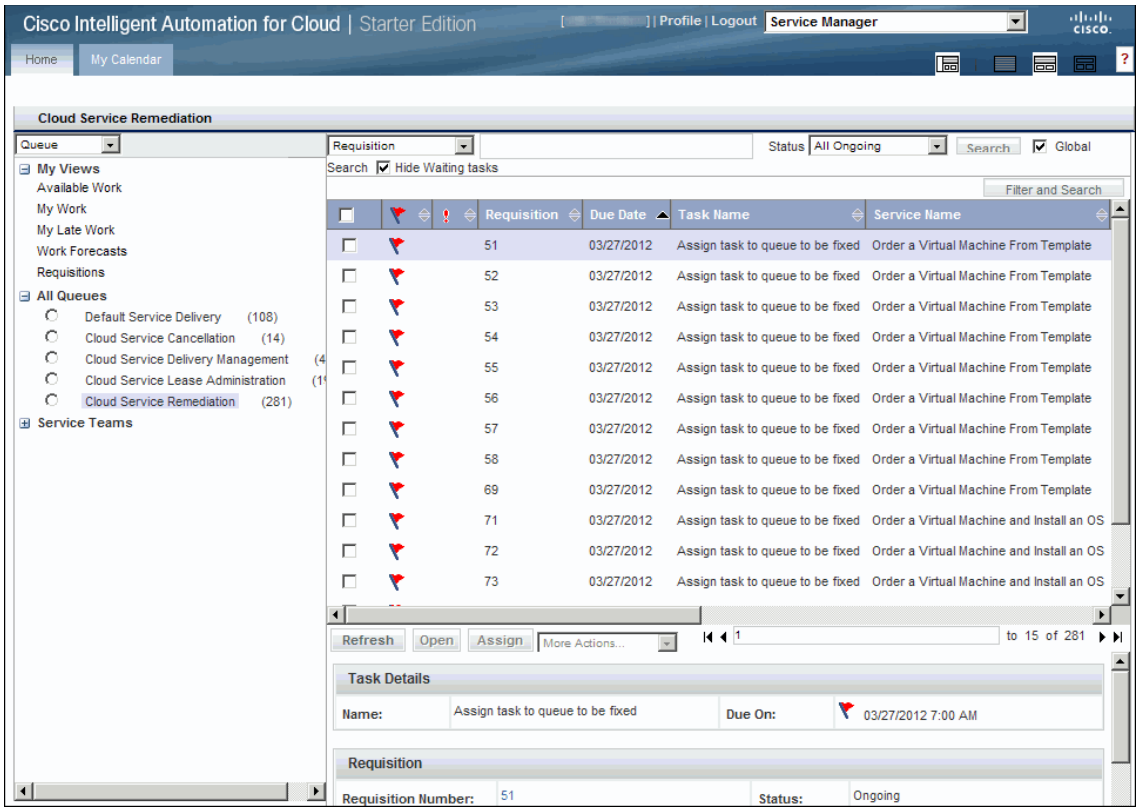
View the Cloud Service Remediation queue and assign a task using the following steps:

Step 1 Choose **Service Manager** from the module drop-down list.

Step 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* **Cloud Service Remediation**.

Unassigned tasks appear in a list.

Figure 5-4 Service Manager—Cloud Service Remediation Queue



Tip You can change the view of the tables in Service Manager using buttons located on the right-hand side under the module drop-down list. Click to show or hide the tree. Click to hide the tree, preview panels, and show only the list. Click (default view) to show a split view list and preview panels, without the tree. Click to show the preview panels only. Service Manager does not save your views.

Step 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 list.

Step 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 selected person's My Work view; the person is notified of the assignment.

After the task is assigned, the assignee must first check out the task from the Cloud Service Remediation queue before fixing the failure. Proceed to Remediating a Service.

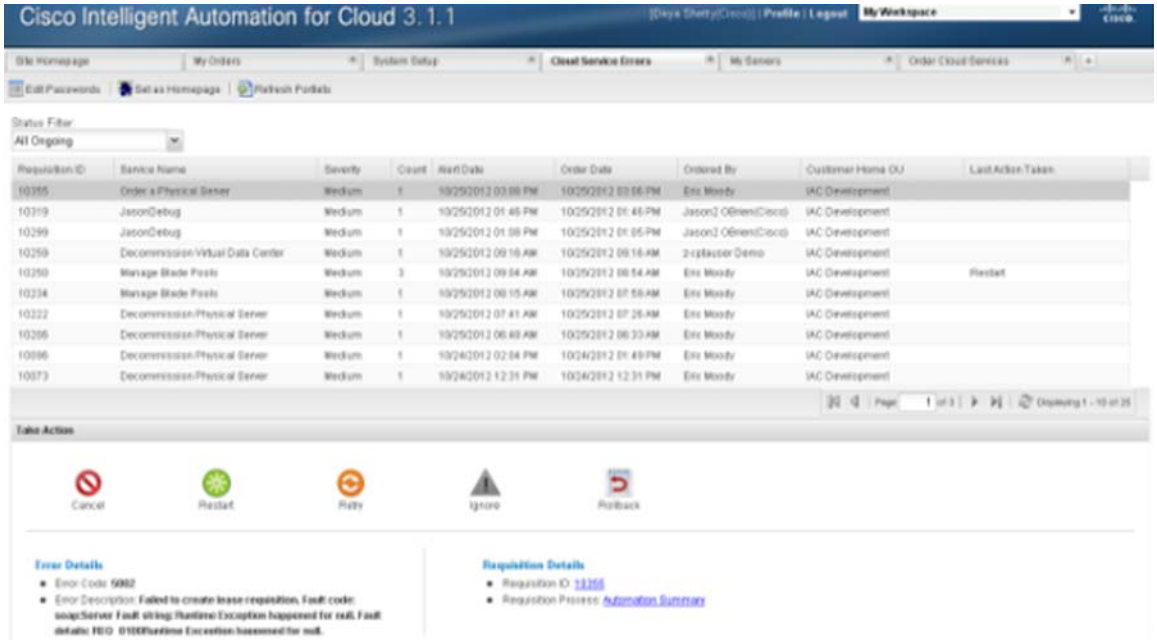
Remediating a Service

After you have checked out the task (see Assigning the Remediation Task for Repair) from the Cloud Service Remediation queue, you then remediate the issue and initiate continuation of the fulfillment process.

Caution To free up the reserved resources, you *must* attempt to remediate the issue, even if you know or suspect the attempt will fail. **Do not cancel the order unless your attempt to remediate the issue is unsuccessful**.

Step 1 Choose **My Workspace** from the module drop-down list, then click **Cloud Service Errors** tab.

The table displays information such as requisition ID, the name of the service that has encountered errors, the severity of the error, the date when the service was ordered, and the last action taken on the service.



Step 2 Select the service that is assigned to you and needs action.

Step 3 You may choose one of the following options available on the **Take Action** panel to remediate the service.

- Retry 

- Retry option is 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 

- Ignore option 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 

- Rollback option is 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. Therefore the service could be at its starting point after a Rollback and you could continue to create a new order.

- Restart 

- Restart option is available for every service. This action will undo any changes to the service and attempts to start over from the beginning of the order. For example, a service “Commission Physical Server” fails because the server provisioner TFTP service is not functioning. You could do a complete rollback and start the process again.

- Cancel 

- Cancel option 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

Step 4 Perform the necessary steps to remediate the issue.

Step 5 After remediating the issue, click **Submit Order**.This action changes the status of the task to I*n 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.

If the delivery process is *not* successful, the requisition will appear in the Cloud Service Cancellation queue. Skip to Cancelling the Order if Remediation Attempt is Unsuccessful, page 5-11.

Checking the Status of an Order

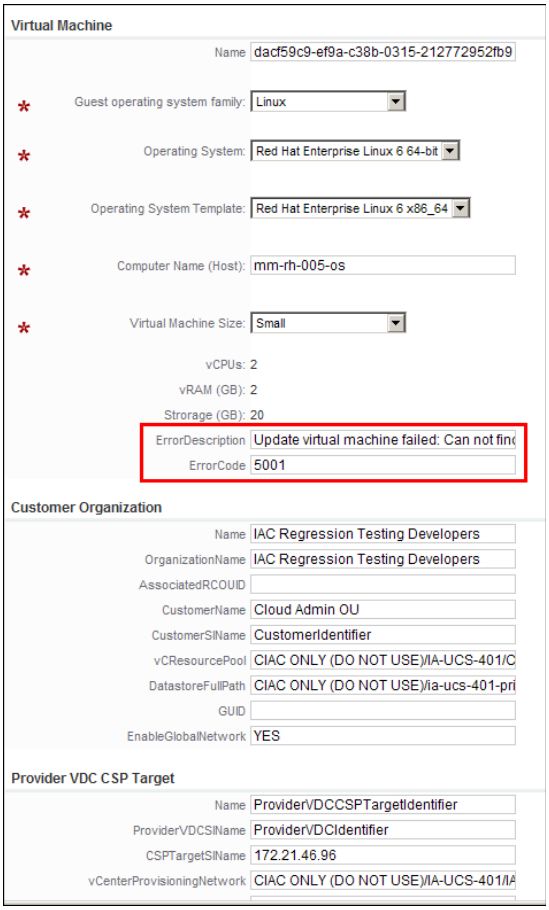
If the delivery process is successful, then the ordered service will be fulfilled and the requisition status changed to Complete, and no further action is needed. To check the status:

Step 1 Return to the Service Manager Home page and click **Cloud Service Delivery Management** under All Queues in the left-hand panel.

Step 2 Locate the requisition in the queue, then click the requisition number to open the Task Data page.

The status is listed in the Service Information panel.

Figure 5-5 Service Manager—Task Data



Cancelling the Order if Remediation Attempt is Unsuccessful

Caution To free up the reserved resources, you *must* attempt to remediate the issue before cancelling the order, as instructed in Remediating a Service, 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.

Step 1 On the Service Manager Home page, click **Cloud Service Cancellation** under All Queues in the left-hand panel.

Step 2 Locate the requisition in the queue, then click the requisition number to open the Task Data page.

Step 3 Click **Cancel**. This action terminates the order and change service status to Cancel.

INDEX

S

T

U

V