



Cisco Intelligent Automation for Cloud Configuration Guide

Release 3.1
November 4, 2012

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-27671-01

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

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

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

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

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

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

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

Cisco Intelligent Automation for Cloud 3.1 Configuration Guide
© 2012 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface 9

- Organization 9
- Conventions 11
- Product Documentation 12
 - Documentation Formats 12
 - Guides and Release Notes 12
 - Online Help 12
 - Product Naming Conventions 12
- Obtaining Documentation and Submitting a Service Request 13

CHAPTER 1

Solution Prerequisites 1-1

- Minimum System Requirements 1-2
 - Minimum Hardware Requirements for Platform Elements 1-2
 - Minimum Software Requirements 1-3
- Default Ports and Protocols 1-4
- Limitations and Scalability 1-5
- Customer Environment 1-6
 - Intelligent Automation for Cloud Software Installation Preparation 1-6
 - Networks 1-7
 - Storage Management Preparation 1-7
 - Cisco UCS and Bare Metal Operating System Provisioning Preparation 1-7
 - Cisco UCS Manager 1-8
 - Cisco UCS Manager Pools 1-8
 - Cisco UCS Manager Service Profile Templates and Policies 1-8
 - VMware Software Preparation 1-9
 - Directory and Mail Server Preparation 1-10
 - Organizations and Users Preparation 1-10

CHAPTER 2

Configuring Cisco Tidal Enterprise Orchestrator and Deploying Cisco Intelligent Automation for Cloud Content 2-1

- Import the Automation Packs in Tidal Enterprise Orchestrator 2-2
 - Launch the Automation Pack Import Wizard 2-2
 - Import the Core Automation Pack 2-3
 - Import the Common Activities Automation Pack 2-8

- Import and Configure the Intelligent Automation for Compute Automation Pack 2-9
- Import and Configure the Intelligent Automation for Cloud Starter Automation Pack 2-14
- Import and Configure the Intelligent Automation for Cloud Automation Pack 2-21
- Setup for Cloud Portal on Linux 2-22
 - Configure Extended Target Properties for Cisco Cloud Portal Integration API 2-23
 - Create a Runtime User for the Linux Target 2-23
 - Create a Target for the Linux Server 2-24
 - Configure the Extended Target Properties for Both Cloud Portal Web Service Targets 2-25
 - Configure Extended Target Properties for Cisco Cloud Portal Request Center API 2-25
- Setup for Tidal Enterprise Orchestrator Server Web Service 2-26
 - Setup for Internet Information Services 2-26
 - Refresh Server Web Service 2-27

CHAPTER 3

Installing the REX Adapter 3-1

- Prerequisites 3-2
- Apply the Cloud Portal Patch 3-2
- Install the REX Adapter 3-2

CHAPTER 4

Configuring Cisco Cloud Portal and Deploying Cisco Intelligent Automation for Cloud Content 4-1

- Enable Web Services 4-2
- Create a Dropbox for Data Synchronization 4-3
- Import and Deploy Intelligent Automation for Cloud Service Catalogs 4-3
 - Copy Service Catalog Files to Cloud Portal Server 4-4
 - Import and Deploy Service Catalogs 4-4
- Import and Deploy Portal Packages 4-5
 - Copy the Cisco IAC Portlets Package and Extract Files 4-5
 - Configure Cloud Portal Stylesheets 4-6
 - Import and Deploy Portal Pages 4-8
- Modify Maximum Numbers for Tabs, Portals, and Portlets 4-9
- Modify Column Settings for the Site Homepage 4-11
- Set Permissions for Portals and Portlets 4-12
 - Set Permissions for the MyWorkspace Portal Pages 4-12
 - Set Permissions for Portlets 4-14
- Adding the Approvals Portlet to the My Approvals Portal Page 4-16
- Adding the OrderStatus Portlet to the My Orders Portal Page 4-16
- Adding Portal Pages to My Workspace 4-17

Assign Additional Permissions for the Cloud Provider Technical Administrator Role	4-17
Set Read/Write Permissions for Organization Unit, Person, and Queue	4-18
Set Read Permissions for Managing Other Roles	4-18
Set Permissions for Service Queue Management	4-20
Assign Additional Permissions for the Organization Technical Administrator Role	4-22
Assign Read Permissions for Role	4-22
Assign Read Permissions for Person	4-22
Assign Additional Permissions for the Server Owner Roles	4-23
4-23	

CHAPTER 5

Running the Configuration Wizard 5-1

Prerequisites	5-2
Overview	5-2
Getting Started	5-2
Step 1: Agent Properties Configuration	5-4
Step 2: Cloud Administration	5-5
Step 3: Connect Cloud Infrastructure	5-6
Step 4: POD Management	5-7
Step 5: Set System-Wide Services and Provisioning Settings	5-8
Step 6: Add Networks (Optional)	5-9
Step 7: Create Shared Zone (Optional)	5-10
Setup Complete	5-11

CHAPTER 6

Creating Cloud Administration Organization and Administrative Accounts 6-1

Set Up REX and nsAPI User Accounts	6-2
Configure Agent Properties	6-5
Set Username and Password for REX Set REX Agent Properties	6-6
Start the REX Set Agent Properties Agent	6-7
Set REX Agent Configuration	6-7
Start the REX Set HTTP Properties Agent	6-8
Set HTTP Agent Configuration	6-9
Start All Other Agents	6-10
Assign Mail Addresses for Queue Notifications	6-10
Configure the Email Notification Templates	6-12
Create the Cloud Provider Technical Administrator Organization	6-15
Add Cloud Provider Technical Administrators	6-15
Add Cloud Administrators in the Directory Service (If Applicable)	6-16

Manually Add Cloud Administrators (Without Directory Service) 6-16
 Manually Make nsAPI a Cloud Administrator (Without Directory Service) 6-17
 Manually Add Site Administrator Role to nsAPI user (Without Directory Service) 6-18
 Configure and Enable Approvals 6-18

CHAPTER 7

Setting Up the Cloud Infrastructure 7-1

Connect the Cloud Platform Elements 7-2
 Define the VMware vCenter Server Platform Element 7-2
 Define the Cisco UCS Manager Platform Element 7-3
 Define the Cisco Server Provisioner Platform Element 7-5
 Set Provisioning Settings 7-6
 Set System-wide Service Options 7-7
 Stop and Start CIM Agents 7-10
 Remediating a Platform Element Discovery Error 7-10
 Create One or More PODs 7-11
 Register a Datastore 7-12
 Set Up a Shared Zone 7-13

CHAPTER 8

Post-Configuration Options 8-1

Managing Server Templates 8-1
 Registering a Virtual Machine Template 8-1
 Registering an Operating System Template 8-2
 Registering a UCS Service Profile Template 8-3
 Manage Blade Pools 8-5
 Modify Standards for Service Options 8-7
 View Standards Settings 8-7
 Add, Modify, or Delete a Lease Term Standard 8-8
 Add a New Lease Term Standard 8-8
 Modify a Lease Term Standard 8-10
 Delete a Lease Term Standard 8-11
 Add, Modify, or Delete an Operating System Standard 8-11
 Add an Operating System Standard 8-11
 Modify an Operating System Standard 8-12
 Delete an Operating System Standard 8-12
 Add, Modify, or Delete a Server Size Standard 8-13
 Add a Server Size Standard 8-13
 Modify a Server Size Standard 8-14
 Delete a Server Size Standard 8-14

Add, Modify, or Delete a VDC Size Standard	8-15
Add a VDC Size Standard	8-16
Modify a VDC Size Standard	8-17
Delete a VDC Size Standard	8-18
Planning VDC Package Sizing	8-18
Add Additional Networks	8-21
Inactivate Reserved Portlet Buttons from the My Workspace Toolbar	8-23

CHAPTER 9

Setting Up an Organization and Adding Users	9-1
Create an Organization	9-2
Set Up Directory Integration (If Applicable)	9-2
Create a New User to Add as an Organization Technical Administrator	9-3
Add a Server Owner	9-4
Assign Mail Addresses for Queue Notifications	9-5

CHAPTER 10

Upgrading to Cisco Intelligent Automation for Cloud 3.1	10-1
Upgrade Prerequisites	10-2
Differences Between Cisco Intelligent Automation for Cloud Starter Edition and Cisco Intelligent Automation for Cloud 3.1	10-2
Supported Upgrade Scenarios	10-3
Actions Performed by the Upgrade Process	10-4
Upgrade to Cisco Intelligent Automation for Cloud 3.1	10-5
Back Up the Cloud Portal and TEO Databases	10-6
Deploy the TEO 2.3.4 Content Update	10-6
Verify the Intelligent Automation for Cloud 3.1 Upgrade Prerequisites	10-6
Apply the Cisco Cloud Portal 9.4 Patch	10-8
Upgrade the REX Adapter	10-8
Deploy Cisco IAC CP Upgrade Content	10-8
Deploy Service Catalog Packages	10-8
Deploy Portal Packages	10-9
Set Permissions for Portals and Portlets	10-9
Set Permission for Upgrade Wizard Portal Page	10-9
Configure Contact Information for Service Queue Notifications	10-9
Configure the Email Notification Templates	10-10
Set Permissions for the Roles Groups	10-10
Change the Home Organization Unit of the nsAPI User	10-10
Configure Agent Properties	10-10
Run Discovery	10-11

Register Discovered Resources 10-12
 Run the Upgrade Wizard 10-12
 Remove the Starter Edition Portal Pages 10-14

APPENDIX A

Setting Up Directory Integration A-1

Prerequisites A-2
 Introduction A-2
 Step 1: Configuring the LDAP Server A-3
 Step 2: Configure Authentication A-5
 Configure Mappings A-5
 Configure Events A-6
 Step 3: Configure Authorization (Optional) A-8
 Create a Security Group for Each User Role on the LDAP Server A-8
 Add the nsAPI User to the Cloud Administration Group A-9
 Configure User Role Mappings A-9
 Step 4: Enable Directory Integration A-9

APPENDIX B

Solution Prerequisites Checklists B-1

Minimum Hardware Requirements for Platform Elements B-2
 Minimum Software Requirements B-3
 Default Ports and Protocols B-4
 Limitations and Scalability B-5
 Cisco IAC Software Installation Preparation B-5
 Network Requirements B-6
 Storage Management Requirements B-6
 Cisco UCS Manager and Bare Metal Operating System Provisioning Requirements B-7
 VMware Software Requirements B-8
 Directory and Mail Server Requirements B-8
 Organizations and Users Preparation B-9
 Create a Virtual Datacenter B-9
 Create Shared Zones B-9
 Order VM From Template B-9
 Order a VM and Install an Operating System B-10
 Order a Physical Server B-10
 Provision ESXi B-10

APPENDIX C

Solution Deployment Checklists	C-1
Cisco Intelligent Automation for Cloud Prerequisites	C-2
Tidal Enterprise Orchestrator Setup Checklist	C-2
REX Adapter Installation Checklist	C-2
Directory Integration Setup Checklist (If Applicable)	C-3
Cloud Portal Setup Checklist	C-3
Service Catalog Deployment Checklist	C-4
Portal and Portlet Deployment Checklist	C-4
Permissions Settings for Portal and Portlets Checklists	C-5
Configure and Enable Approvals Checklist	C-6
Configuration Wizard Checklist (Optional)	C-7
Cloud Administration Setup Checklist	C-8
Email Notification Template Modification Checklist	C-9
Cloud Infrastructure Setup Checklist	C-10
Organizations and Users Setup Checklist	C-10
Directory Integration Setup Checklist (If Applicable)	C-11

APPENDIX D

Solution Deployment Worksheets	D-1
Hardware Specifications	D-2
Software Specifications	D-3
Database Connection Settings	D-4
TEO Web Service Target Settings	D-5
TEO-Cloud Portal Integration API Connection User Account Credentials	D-5
Cisco Service Portal Request Center and Service Link User Account Credentials	D-5
REX Adapter Installation Settings	D-6
Directory Integration Settings (If Applicable)	D-7
LDAP Server Configurations	D-7
Configure Authentication	D-7
Configure Mapping	D-7
Configure Events	D-8
Mappings Settings	D-8
Events Settings	D-8
Cloud Administrator and Organization Settings	D-9
Agent Properties Settings	D-9
REX Set REX Agent Configuration Settings	D-9
REX Agent Configuration Settings	D-10

- Set HTTP Properties Configuration Settings D-10
- Email Addresses for Queue Notifications D-11
- Cloud Platform Connection Settings D-11
 - VMware vCenter Server Connection Settings D-11
 - Cisco UCS Manager Connection Settings D-12
 - Cisco Server Provisioner Connection Settings D-12
- Provisioning Settings D-13
- System-wide Service Options D-13
- Network Settings D-14
- POD Settings D-14
- Shared Zone Settings D-15
- Standards Settings (Optional) D-15
 - Lease Term Standards D-15
 - Operating Systems Standards D-16
 - Server Size Standards D-17
 - VDC Size Standards D-18



Preface

The *Cisco Intelligent Automation for Cloud 3.1 Configuration Guide* provides instructions for configuring Intelligent Automation for Cloud (Cisco IAC). It includes information about preparing your environment with the prerequisite application servers and software, installing the Cisco IAC content, configuring Cisco Cloud Portal and setting up your cloud environment.

Organization

This guide includes the following sections:

Chapter 1	Solution Prerequisites	Provides information about preparing your environment with the prerequisite servers and software prior to installing Cisco Intelligent Automation for Cloud 3.1 (Cisco IAC). Note You must review this chapter in its entirety before installing Cisco IAC to ensure that all requirements are fulfilled. Use the checklists in Appendix C, “Solution Deployment Checklists” to ensure that your environment meets all requirements.
Chapter 2	Configuring Cisco Tidal Enterprise Orchestrator and Deploying Cisco Intelligent Automation for Cloud Content	Guides you through the necessary tasks to import Automation Packs into Tidal Enterprise Orchestrator and set extended target properties for Linux (if applicable).
Chapter 3	Installing the REX Adapter	Provides instructions for installing the required REX adapter.
Chapter 4	Configuring Cisco Cloud Portal and Deploying Cisco Intelligent Automation for Cloud Content	Guides you through the necessary tasks to prepare Cisco Cloud Portal for configuration, deploying service catalogs, and deploying portal pages.

Chapter 5	Running the Configuration Wizard	Guides you through setting up and configuring vital components of Cisco Intelligent Automation for Cloud Cisco IAC. It saves you time by providing access to the various forms and services from one location
Chapter 6	Creating Cloud Administration Organization and Administrative Accounts	Provides steps for establishing the Cloud Provider Technical Administrator home organization and adding Cloud Provider Technical Administrators.
Chapter 7	Setting Up the Cloud Infrastructure	Provides steps for setting up platform elements for VMware vCenter Server™, Cisco Unified Computing System™ (UCS) Manager, and Cisco Server Provisioning; adding networks; and setting up a shared zone.
Chapter 8	Post-Configuration Options	Provides steps for optional tasks, such as adding additional templates and networks, registering Cisco UCS blades, and modifying standards.
Chapter 9	Setting Up an Organization and Adding Users	Guides you through creating an organization, assigning an Organization Technical Administrator, assigning permissions, and adding Server Owners.
Chapter 10	Upgrading to Cisco Intelligent Automation for Cloud 3.1	Shows you how to upgrade from Cisco IAC Starter Edition 3.0.2 on Cisco Cloud Portal 9.4 to Cisco Intelligent Automation for Cloud 3.1 on Cloud Portal 9.4.
Appendix A	Setting Up Directory Integration	Provides instructions for integrating your directory service into Cisco IAC. Note Refer this appendix only if you are using a directory service to import user and organization information.
Appendix B	Solution Prerequisites Checklists	Provides a means for ensuring that your environment meets all of the requirements for setting up and using Cisco IAC.
Appendix C	Solution Deployment Checklists	Guides you through each step in the configuration process. The checklists include each set of instructions in this guide, in sequence, that you check off as you move along. It is strongly recommended that you utilize the checklists.
Appendix D	Solution Deployment Worksheets	Provides logs for the settings you specify as you configure Cisco IAC. It is strongly recommended that you fill out the worksheets completely and save them for Cisco Services or other administrators to reference in the event that problems arise.

Conventions

This guide uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in bold font .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
[]	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.
<code>courier font</code>	Terminal sessions and information the system displays appear in <code>courier font</code> .
< >	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**.

Product Documentation

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 Web site at www.adobe.com.

Guides and Release Notes


You can download the following documentation for Cisco Intelligent Automation for Cloud from cisco.com:


- *Cisco Intelligent Automation for Cloud 3.1 Release Notes*
- *Cisco Intelligent Automation for Cloud 3.1 Upgrade Guide*
- *Cisco Intelligent Automation for Cloud 3.1 User Guide*

Online Help

Online help is available for Tidal Enterprise Orchestrator (TEO) and Cisco Cloud Portal.

For TEO, 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 TEO 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 Intelligent Automation for Cloud user interface:

- Cisco Service Portal is synonymous with Cisco Cloud Portal.

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.



CHAPTER 1

Solution Prerequisites



Note

Before you begin configuring and deploying Cisco Intelligent Automation for Cloud, you **must** review this entire chapter to ensure that your datacenter infrastructure is properly configured. **If any of the requirements presented in this chapter are not met, deployment might fail.**

This chapter provides information on the required hardware and software that must be installed before for installing and deploying Cisco Intelligent Automation for Cloud (Cisco IAC).

It includes the following sections:

- [Minimum System Requirements](#)
- [Default Ports and Protocols](#)
- [Limitations and Scalability](#)
- [Customer Environment](#)



Note

This chapter provides only product names. For version numbers, see the [Cisco Intelligent Automation for Cloud Product Compatibility Matrix](#).

Minimum System Requirements

Before installing Cisco IAC, it is recommended that you verify that your datacenter infrastructure meets the minimum hardware and software requirements. The requirements in this section provide the minimum prerequisites necessary to install and deploy Cisco IAC.

Minimum Hardware Requirements for Platform Elements

Before Cisco IAC can be installed and deployed, all of the required hardware and virtual server resources presented in [Table 1-1](#) must be installed and configured according to the documentation that shipped with the products.

Table 1-1 Minimum Hardware Requirements for Platform Elements

Platform Element	Component	Client	Server
Tidal Enterprise Orchestrator (TEO) Server ¹	CPU	2.8 GHz or higher core (Dual core systems recommended)	64-bit 2.8 GHz or higher core (Quad core systems recommended)
	Memory	2 GB minimum (4 GB or higher recommended)	2 GB minimum (8 GB or higher recommended) 8 GB of RAM (if Microsoft SQL Server is installed on same machine as TEO) It is recommended that the database reside on a separate server.
	Disk Space	1 GB dedicated to TEO (2 GB or higher recommended) ²	1 GB of available hard disk space dedicated to TEO (2 GB or higher recommended) ²
Cloud Portal	CPU	—	Intel Core 2 Dual processor or equivalent
	Memory	—	4 GB RAM
	Disk Space	—	40 GB free hard disk space
Cloud Portal Database	CPU	—	Intel Core 2 Dual processor or equivalent
	Memory	—	4 GB RAM
	Disk Space	—	50 GB free hard disk space ³
Cisco Server Provisioner	CPU	—	EM64T, Intel 64, or AMD64
	Memory	—	512 MB
	Disk Space	—	40 GB ⁴

1. For complete installation prerequisites, see the *Tidal Enterprise Orchestrator Installation and Administration Guide* on [Cisco.com](#).
2. For disk space sizing formula, see the *Tidal Enterprise Orchestrator 2.4 Installation and Administration Guide* on [Cisco.com](#).
3. Disk space requirement is dependent on the projected size of your Service Portal databases over time, to account for the growth in user data, service definitional data, transactional data, and reporting data.
4. For additional information on scoping disk space, see the [Cisco Server Provisioner documentation](#) on LinMin.com.

Minimum Software Requirements

Before Cisco IAC can be installed and deployed, all of the required software presented in [Table 1-2](#) must be installed and configured according to the documentation that shipped with the products.



Note

See the [Cisco Intelligent Automation for Cloud Product Compatibility Matrix](#) for the supported versions.

Table 1-2 Minimum Software Requirements

Component	Server	Requirement
Application Server Operating System	TEO	Microsoft Windows Server ¹
	Cloud Portal	Microsoft Windows Server ¹ Red Hat Enterprise Linux ¹
	Cisco Server Provisioner	Red Hat or CentOS ¹
Application Server Framework	TEO	.NET Framework ¹ VMware vSphere PowerCLI ¹
	Cloud Portal	JBoss® ¹
Application Software	TEO	TEO ¹
	Cloud Portal	Cloud Portal ¹ Cloud Portal patch ¹ REX adapter
LDAP Server	TEO	Microsoft Active Directory ¹
	Cloud Portal	Microsoft Active Directory ¹ IBM Tivoli™ Directory Server ¹ Sun Java™ System Directory Server ¹ Note For Cloud Portal, you must create the six user groups in the directory: Cloud Provider Technical Administrator, Field Extender, Organization Technical Administrator, Solutions Team, Virtual Server Owner, and Virtual and Physical Server Owner. These user groups will serve as containers for identifying user role assignments. The user groups must be named according to the role name in Cloud Portal. Consult the documentation that came with your directory software for instructions on setting up user groups.
Web Server	TEO	Microsoft Internet Information Services (IIS) ¹
	Cloud Portal	Microsoft Internet Information Services (IIS) ¹
Database	Process Orchestrator	Microsoft SQL Server ¹ Oracle® Database Enterprise Edition ¹
	Cloud Portal	Microsoft SQL Server ¹ Oracle Database Enterprise Edition ¹

Table 1-2 Minimum Software Requirements (continued)

Component	Server	Requirement
Web Browser	TEO	Microsoft Internet Explorer ¹ Mozilla Firefox ¹
	Cloud Portal	Microsoft Internet Explorer ¹ Mozilla Firefox ¹
Virtualization ²	Hypervisor ³	VMware ESXi ¹
	Hypervisor Manager	VMware vCenter/vSphere ¹
Physical Server Provisioning	Cisco UCS Manager	Cisco UCS blades ¹

1. See the [Cisco Intelligent Automation for Cloud Product Compatibility Matrix](#) for the supported version or versions.
2. For Cisco IAC, vCenter object names cannot contain forward slashes. For more information, please see [VMware Software Preparation, page 1-9](#).
3. For specific ESXi/vCenter compatibility, refer to interoperability guidelines on VMware.com.

Default Ports and Protocols

This section provides the default ports used by Cisco IAC.



Note

Ensure that the network ports are open in any firewalls that protect the servers where the software platforms are installed.

Table 1-3 Requirements—Cisco IAC Ports and Protocols

Application	Default Port	Protocol	Description
Cloud Portal	8080	TCP	Client web browser connections to the Cloud Portal RequestCenter
	8080	TCP	TEO communications to the Cloud Portal inbound web service
TEO	2081	TCP	User Web browser connections to the TEO web console
	61525	TCP	TEO Console access to the TEO Server
	61526	TCP	Web Service (API) communication using HTTPS protocol from the Cloud Portal to the TEO web service.
	61527	TCP	Web Service (API) communication using HTTP protocol from the Cloud Portal to the TEO web service.

Table 1-3 Requirements—Cisco IAC Ports and Protocols (continued)

Application	Default Port	Protocol	Description
Cisco Server Provisioner ¹	80	TCP	HTTP web service communication between TEO and Cisco Server Provisioner
	21	TCP	FTP protocol used for Cisco Server Provisioner client provisioning
	67	UDP	BOOTP protocol used for Cisco Server Provisioner client provisioning.
	111	UDP	TFTP protocol used for Cisco Server Provisioner client provisioning
	139	TCP/UDP	NetBios protocol used for Cisco Server Provisioner client provisioning
	445	TCP/UDP	SMB protocol used for Cisco Server Provisioner client provisioning
	4011	TCP	BINL protocol used for Cisco Server Provisioner client provisioning

1. For additional information, see the [Cisco Server Provisioner User Documentation](#) on Cisco.com.

Limitations and Scalability

Cisco IAC enforces the limitations for performance and scalability as listed in [Table 1-4](#).

Table 1-4 Requirements—Cisco IAC Limitations and Scalability

Entity	Limitations
TEO server	1 server
Registered users	Up to 1,000; up to 200 concurrent users
Service items (concurrent)	Up to 10,000
VMware vCenter ¹	1 instance

1. For Cisco IAC, vCenter object names cannot contain forward slashes. For more information, please see [VMware Software Preparation, page 1-9](#).

Customer Environment

To ensure a successful installation of Cisco IAC, customers should perform the tasks in the following sections to prepare their environment prior to installing Cisco IAC.

- [Intelligent Automation for Cloud Software Installation Preparation, page 1-6](#)
- [Networks, page 1-7](#)
- [Storage Management Preparation, page 1-7](#)
- [Cisco UCS and Bare Metal Operating System Provisioning Preparation, page 1-7](#)
- [VMware Software Preparation, page 1-9](#)
- [Directory and Mail Server Preparation, page 1-10](#)
- [Organizations and Users Preparation, page 1-10](#)

Intelligent Automation for Cloud Software Installation Preparation

Prepare your environment by installing prerequisite software.

- Prepare application servers by installing the operating system (including software prerequisites such as .NET framework, Java, JBoss) on the following solution components:
 - TEO
 - Cloud Portal
 - Cisco Server Provisioner
- Install database management servers that are available to following solution components:
 - TEO
 - Cloud Portal
- Install each of the following:
 - TEO on a targeted application server—See the *Tidal Enterprise Orchestrator Installation and Administration Guide* on [Cisco.com](#).
 - Cloud Portal on a targeted application server—See the *Service Portal System Administrator Guide* on [Cisco.com](#)
 - Cisco Server Provisioner on a targeted application server—See the *Cisco Server Provisioner User's Guide* on [LinMin.com](#).

Networks

Prepare your networks to include the following requirements:

- At least one VLAN to use as a destination network for provisioning servers. You can define a destination network as a community, user, or management network when you create the network in Cloud Portal.
 - Community networks are used by the shared zone and any server owner can provision servers to the shared zone.
 - User networks are assigned to specific Virtual Data Centers owned by an organization.
 - Management networks within the cloud system may be used to manage cloud servers, for example, for remote access and monitoring.
- Optional: A private VLAN for use by Cisco Server Provisioner for server deployment. This is only needed if any of the following features are enabled: Virtual Machine and Install OS Ordering, Physical Server Ordering, ESXi Provisioning.
- Optional: A VLAN to use as a destination network for ESXi hosts. This infrastructure network represents the management network the host will use to communicate with your vCenter Platform Element. This is only needed if the ESXi Provisioning feature is enabled.

Storage Management Preparation

Prepare your storage management system using the following checklist and information:

- Install and configure SAN storage or iSCSI storage required for DRS clusters. For iSCSI or NFS storage solutions, VMware¹ supports DHCP. It is important that any of these solutions use DHCP, otherwise static IP information, wherever it is applicable, will have to be configured manually after the automated process is complete.
- Create the storage volumes that will be used for the datastore clusters.
- Configure LUN access in your storage management system and assign WWN pools (*see Cisco UCS Manager Pools, page 1-8*)

vCenter datastores map to or reference specific LUNs. These mappings will replicate to a new host if the host blade has been given the same LUN access as all the other hosts in the cluster. This is accomplished through WWN pools.

LUN configuration can be assigned to any WWN that is within a specific range. For a new host to be assigned WWNs that are within that range, ensure that it is coming from the pre-defined pool. Whenever a service profile is created from a service profile template for a blade, specify that the template generate WWN assignments from a specific pre-defined pool in Cisco UCS Manager. Datastore access should be automatically be in sync with all the other hosts in that cluster when the service profile template is used to provision the blade.

Cisco UCS and Bare Metal Operating System Provisioning Preparation

Prepare your Cisco UCS environment according to requirements for the following:

- [Cisco UCS Manager](#)

1. For the supported VMware version, see the [Cisco Intelligent Automation for Cloud Product Compatibility Matrix](#).

- [Cisco UCS Manager Pools](#)
- [Cisco UCS Manager Service Profile Templates and Policies](#)

Cisco UCS Manager

Cisco UCS Manager must be installed and configured before installing Cisco IAC.



Note

For instructions on installing and configuring the application, see [Cisco UCS Manager documentation](#) on Cisco.com.

Cisco UCS Manager Pools

Cisco UCS Manager utilizes different types of pools to control assignment of unique identifiers (such as UUIDs, MACs and WWNs) to blade servers. These pools must be created and assigned to Service Profiles.

You must create the following pools:

- **UUID Suffix Pool**—Used to uniquely identifies each blade server.
- **MAC Address Pool**—Used to assign a unique MAC address to each vNIC assigned to a blade.
- **WWNN (World Wide Node Name) Pool**—Assigned to a node in a Fibre Channel fabric, and used to assign unique WWNNs to each blade in a range that will allow appropriate LUN access
- **WWPN (World Wide Port Names) Pool**—Assigned to specific ports in a Fibre Channel fabric, and used to assign unique WWPNs to each blade in a range that will allow appropriate LUN access



Note

For instructions on creating the pools, see [Cisco UCS Manager documentation](#) on Cisco.com.

Cisco UCS Manager Service Profile Templates and Policies



Note

This is only needed when the Physical Server Ordering or ESXi Provisioning options are enabled in [Set System-wide Service Options, page 7-7](#).

Cisco UCS service profile templates are used for duplicating or deploying multiple UCS service profiles with the same configuration. By associating pools with a template, you ensure that a WWN or MAC Address, for example, will always be within a pre-specified range.

Cisco recommends that a separate service profile template be created for each vCenter cluster.



Caution

For Cisco IAC, vCenter object names cannot contain forward slashes. For more information, please see [VMware Software Preparation, page 1-9](#).



Note

When you register a service profile template through the Templates portal, you will be prompted to associate it with a vCenter cluster if you have selected it to be a Hypervisor template.

The templates must meet the following requirements:

- At least one hypervisor service profile template for each vCenter cluster with the same quantity and configuration of vNICs as on other hosts in the same cluster. The native VLAN for the first vNIC should be set to the Management VLAN for that vCenter.



Note This is only required for ESXi.

- At least one service profile template for physical server provisioning
- A local boot policy assigned to the physical server service profile template which is set to boot to local disk
- A boot policy named **PXEBoot** which is configured to boot from the network.



Note This name is mandatory.

- Provisioning templates are prepared according to Cisco Server Provisioner product documentation. (See the *LinMin Bare Metal Provisioning User's Guide* on LinMin.com.)
- UCS blades for provisioning VMware ESXi hypervisor hosts have at least one local drive.

VMware Software Preparation



Note

This is only needed when the ESCi Provisioning option is enabled in [Set System-wide Service Options, page 7-7](#).



Caution

For Cisco IAC, vCenter object names cannot contain forward slashes. Cisco IAC uses forward slashes as delimiters in object paths and parses vCenter paths by display name. Forward slashes in vCenter object names break the parsing process. If any of your vCenter object names contains forward slashes, please rename the files before you specify a vCenter path.

In Cisco IAC, commissioning a new ESXi host is performed when moving a blade in the Maintenance pool to the Virtual pool. The orchestration process involves provisioning (installing) ESXi on to a blade, adding it to the vSphere infrastructure, copying the configuration from one of the existing hosts in a cluster and applying it to the new host using VMware host profiles and exiting Host Maintenance mode.

Supported installation media for ESXi

Provisioning of the ESXi Hypervisor OS always uses the first local drive installed in the blade. For Cisco IAC, only local installs of the ESXi Hypervisor OS are supported.

VMware Installation Requirements

The following VMware software should be installed:

- vSphere Powershell CLI on the TEO server to support the activities for adding a new ESXi host to a cluster.



Note For supported VMware software versions, see the [Cisco Intelligent Automation for Cloud Product Compatibility Matrix](#).

Prepare your VMware environment for virtual provisioning using the following checklist:

- Install and configure VMware vCenter:
 - Apply enterprise licensing and enable VMware vSphere Distributed Resource Scheduler (DRS).
 - Determine and create the datacenter, clusters, hosts, datastores, networks, and resource pools to which all commissioned hosts and VMs will be deployed.
- Define at least one VM template with VMware tools.



Note Provisioned hosts will have evaluation licensing only. You will need to add licensing manually in the vSphere Client.



Note For information about installing and configuring your VMware environment, see the [ESX and vCenter Server Installation Guide](#).

Directory and Mail Server Preparation

To prepare your directory and email environment, ensure that the following conditions are met:

- LDAP server, Microsoft Active Directory, is installed and configured.



Note If you will implement directory integration, Active Directory is required. Use of other LDAP server software, in addition to Active Directory, is optional. For information on other supported LDAP software, see the [Cisco Intelligent Automation for Cloud Product Compatibility Matrix](#).

- SMTP server installed and configured with an account to send and receive emails.



Note For information on configuring the SMTP server, see the [Cisco TEO 2.3 Installation and Administration Guide](#) or the [Cisco Service Portal Installation Guide](#).

Organizations and Users Preparation

Prepare a list of organizations, organization users, and Organization Technical Administrators to configure in Cloud Portal. For more information about the predefined user roles, their respective capabilities, and how this information can help you plan for your administrator's responsibilities, see the "User Roles and Capabilities" section in the [Cisco Intelligent Automation for Cloud User Guide](#).



CHAPTER 2

Configuring Cisco Tidal Enterprise Orchestrator and Deploying Cisco Intelligent Automation for Cloud Content



Note

Before you can configure and deploy Cisco Intelligent Automation for Cloud, you **MUST** review [Chapter 1, “Solution Prerequisites,”](#) to ensure that your datacenter infrastructure is properly configured and that all of the prerequisite installations of Tidal Enterprise Orchestrator, such as vSphere drop-down list Powershell CLI, are in place. **If any of the requirements presented in this chapter are not met, deployment may fail.**

This chapter guides you through setting up Tidal Enterprise Orchestrator (TEO). It includes the following sections:

- [Import the Automation Packs in Tidal Enterprise Orchestrator](#)
- [Setup for Cloud Portal on Linux](#)
- [Setup for Tidal Enterprise Orchestrator Server Web Service](#)

Import the Automation Packs in Tidal Enterprise Orchestrator

The automation packs are containers of critical automation and portal content for Cisco IAC. There are five automation packs that you must import in TEO:

**Note**

You need to install TEO 2.3.0 and TEO 2.3.4. Both installations offer the option to import automation packs at the end of the install. *Import only the automation packs at the end of the 2.3.4 install.*

1. Core ([page 2-3](#))—Core content, and is a prerequisite for all other automation packs
2. Common Activities ([page 2-8](#))
3. Intelligent Automation for Cloud Compute ([page 2-9](#))
4. Intelligent Automation for Cloud Starter ([page 2-14](#))
5. Intelligent Automation for Cloud ([page 2-21](#))

Launch the Automation Pack Import Wizard

Use the Automation Pack Import Wizard to import the automation packs. The wizard automatically launches after the TEO installation is complete and the automation pack initialization is completed. The wizard does not fully launch until after the TEO service has started.

Use the following steps to import the automation packs immediately after installing TEO.

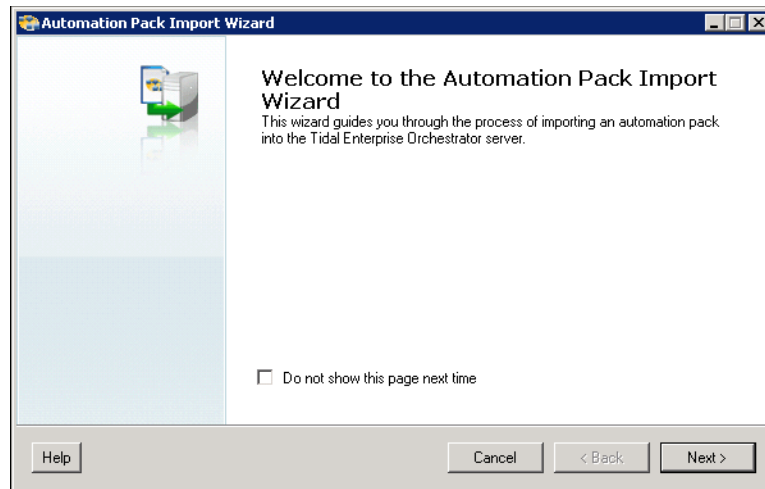
-
- Step 1** Before you close the Setup wizard to complete the installation of the TEO, ensure that the **Launch automation pack import wizard now** check box is checked.
- The Select Automation Packs dialog box displays the available automation packs.
- Step 2** Check the following five check boxes, then click **OK** to launch the Automation Pack Import Wizard:
- a. Core (*Dependency; checked by default*)
 - b. Common Activities (*Dependency*)
 - c. Intelligent Automation for Cloud Compute (*Dependency*)
 - d. Intelligent Automation for Cloud Starter
 - e. Intelligent Automation for Cloud
- Step 3** Proceed to [Import the Core Automation Pack](#).
-

Import the Core Automation Pack

The Core automation pack is the first to import. After you have completed the steps in this section, the wizard will guide you through importing each of the other automation packs.

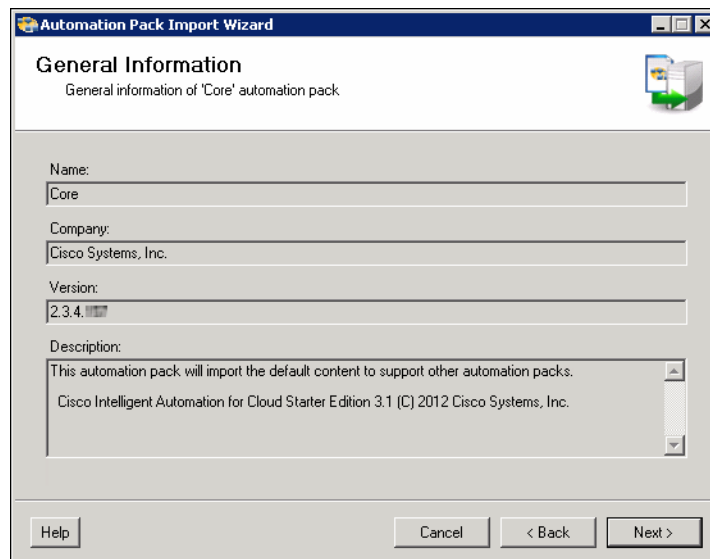
- Step 1** On the Welcome to the Automation Pack Import Wizard panel, review the information, then click **Next**.

Figure 2-1 Automation Pack Import Wizard Welcome Panel



- Step 2** On the General Information panel, review the display-only information about the automation pack, then click **Next** to continue.

Figure 2-2 Automation Pack Import Wizard—Core—General Information



- Step 3** On the Email Configuration panel, provide the default SMTP server and sender's email address to be used for email activities.

Field	Action
Default SMTP server	Enter the name of the SMTP server that is used as the default server for sending email messages.
Default SMTP port	Enter the port number for the SMTP server. This field is automatically populated with port number 25 .
Default sender	Enter the email address of the sender that is designated as the default sender for email activities.

Figure 2-3 Automation Pack Import Wizard—Core—Email Configuration



- Note** You can manually change the settings on this panel when configuring a specific email activity that requires a different SMTP server or sender email address.

- Step 4** Click **Next** to continue.

Figure 2-4 Automation Pack Import Wizard—Core—Automation Summary Configuration

The Automation Summary Configuration panel indicates where the automation summary reports that are generated by activities are to be saved and how long the reports are to be retained. The specified file paths will be used to access and view the automation summary reports.

**Note**

You can access the automation summary from Cloud Portal by mapping the automation summary path to an IIS virtual directory. To enable this option, see [Step 5](#).

Step 5 On the Automation Summary Configuration panel, specify the following information:

Field	Action
Automation Summary Directory	Accept the default directory, or enter a different file path for the automation summary directory. You can also click Browse to navigate to the file path for the automation summary.
Map the automation summary path using	Choose Use IIS Virtual Directory from the drop-down menu to map the automation summary to the file path on an IIS Virtual Directory. Note This IIS Virtual Directory setting is mandatory. In the Virtual directory path field, enter the share folder that corresponds to a virtual directory in IIS. Use the following convention: <code>http://host:(port)/sharefolder</code> . Create your web sites and Virtual Directory in IIS Manager for the share folder. You can use the default settings or change them.
Delete automation summary reports older than	Check this check box, then enter the number of days that the automation summary files should be retained. Automation summary files that are older than the specified number of days will be deleted.

Step 6 Click **Next** to continue.

Figure 2-5 Automation Pack Import Wizard—Core—Default Windows Credentials

Step 7 On the Default Windows Credentials panel, specify the default credentials for the Windows automation server target.

Field	Action
Domain	Enter the name of the domain of the user account that is used to connect to the Windows server.
User name	Enter the username for the user account associated with the server.
Password	Enter the password assigned to the user account.

Step 8 Click **Next** to continue.

Figure 2-6 Automation Pack Import Wizard—Core—Data Extraction


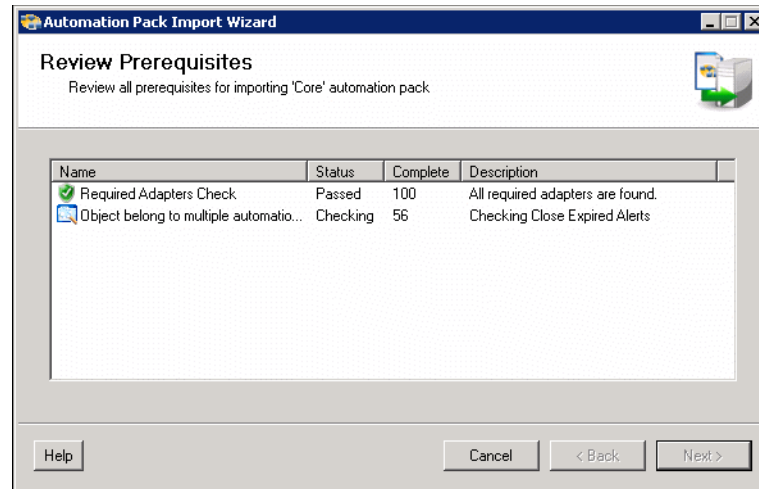
- Step 9** Verify the default location for where the data files should be extracted or click the **Browse**  tool to specify a different location.
- Step 10** Click **Next**.

Figure 2-7 Automation Pack Import Wizard—Core—Review Prerequisites Panel



- Step 11** Click **Next**.

The Review Prerequisites panel displays the prerequisites for the automation pack being imported. The green check mark indicates that the prerequisite was found on the computer.

A red X indicates that the prerequisite was not found on the computer. When this occurs, the import process is stopped and cannot continue until all prerequisites have been met.

If all prerequisites are passed, the wizard automatically continues to the General Information panel for the next automation pack to be imported.

- Step 12** Proceed to [Import the Common Activities Automation Pack](#).
-

Import the Common Activities Automation Pack

The Intelligent Automation for Cloud automation packs have a dependency on the Common Activities automation pack. Therefore, the wizard will guide you through importing this automation pack next.

- Step 1** On the General Information panel, review the information about the automation pack.

Figure 2-8 Automation Pack Import Wizard—Common Activities—General Information

- Step 2** Click **Next** to continue.

Figure 2-9 Automation Pack Import Wizard—Common Activities—Review Prerequisites

Name	Status	Complete	Description
Required Adapters Check	Passed	100	All required adapters are found.
Dependent Automation Packs Check	Passed	100	All dependent automation packs are f...
Object belong to multiple automatio...	Checking	83	Checking Ping

The Review Prerequisites panel displays the prerequisites for the automation pack being imported. The green check mark indicates that the prerequisite was found on the computer.

A red X indicates that the prerequisite was not found on the computer. When this occurs, the import process is stopped and cannot continue until all prerequisites have been met.

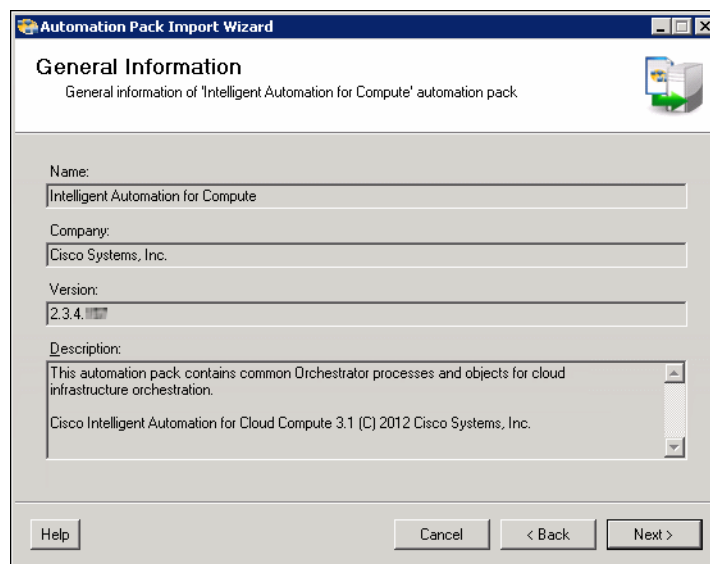
Proceed to [Import and Configure the Intelligent Automation for Compute Automation Pack](#).

Import and Configure the Intelligent Automation for Compute Automation Pack

The Intelligent Automation for Cloud Starter automation pack has a dependency on the Intelligent Automation for Compute automation pack.

Step 1 On the General Information panel, review the information about the automation pack.

Figure 2-10 Automation Pack Import Wizard—Intelligent Automation for Compute—General Information



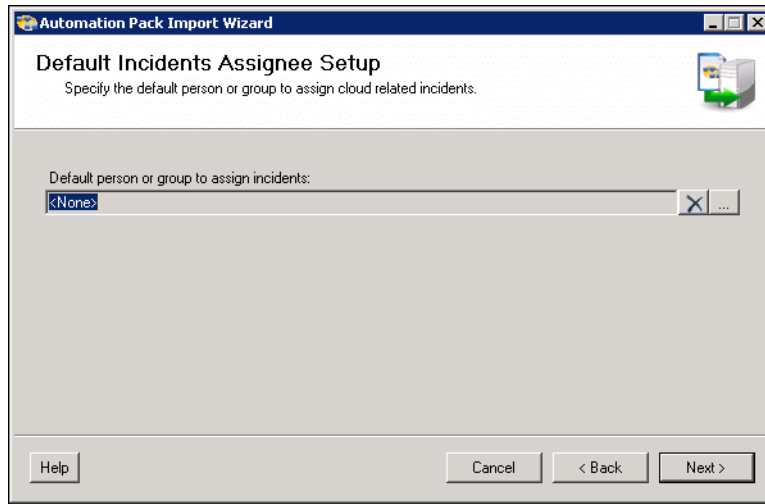
The screenshot shows a window titled "Automation Pack Import Wizard" with a "General Information" tab. The window displays the following information:

- Name:** Intelligent Automation for Compute
- Company:** Cisco Systems, Inc.
- Version:** 2.3.4
- Description:** This automation pack contains common Orchestrator processes and objects for cloud infrastructure orchestration.
Cisco Intelligent Automation for Cloud Compute 3.1 (C) 2012 Cisco Systems, Inc.

At the bottom of the window, there are four buttons: "Help", "Cancel", "< Back", and "Next >".

Step 2 Click **Next** to continue.

Figure 2-11 Automation Pack Import Wizard—Intelligent Automation for Compute—Default Incidents Assignee Setup




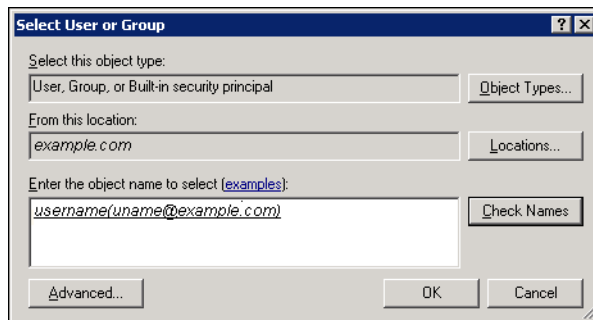
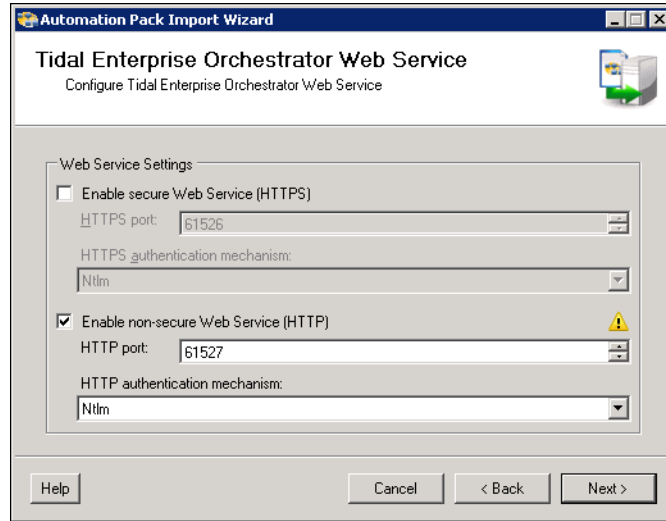
- Step 3** On the Default Incidents Assignee Setup panel, click the **Browse**  tool to specify the default user to assign cloud-related incidents.

Figure 2-12 Automation Pack Import Wizard—Intelligent Automation for Compute—Select User or Group



- Step 4** On the Select User or Group dialog box, click **Location** and choose the location from which the user will be selected.
- Step 5** In the text box, enter the user name and click **Check Names**.
If the name is found, the box will be populated with the appropriate email address.
- Step 6** Click **OK** to close the Select User or Group dialog box.
- Step 7** On the Default Incidents Assignee Setup panel, click **Next** to continue

Figure 2-13 Automation Pack Import Wizard—Intelligent Automation for Compute—Tidal Enterprise Orchestrator Web Service



Step 8 On the Tidal Enterprise Orchestrator Web Service panel, specify the following settings:

Field	Action
Web Service Settings	Check the Enable non-secure Web Service (HTTP) check box. This setting unencrypts the HTTP endpoints.
HTTP Port	Enter or verify the port for the Tidal Enterprise Orchestrator web target.
HTTPS or HTTP authentication mechanism	Choose the appropriate authentication method for the web service: <ul style="list-style-type: none"> • Basic—Standard method that provides a user name and password to the authentication mechanism • Digest—Method that requires parties who are seeking to authenticate to provide their knowledge of secret keys • NTLM—<i>Default</i>. Authentication protocol that is used on networks that include systems running the Windows operating system and on stand-alone systems <p>Note The agents in Cloud Portal must also be set to use the same NTLM authentication that you specify here.</p> <p>Note In IIS, NTLM is not enabled by default. You must enable NTLM in IIS if you choose this authentication mechanism.</p>

Step 9 Click **Next** to continue.

Figure 2-14 Automation Pack Import Wizard—Intelligent Automation for Compute—Tidal Enterprise Orchestrator Web Service Credentials

- Step 10** On the Default Web Service Credentials panel, specify the credentials for connecting to the Tidal Enterprise Orchestrator web service target:

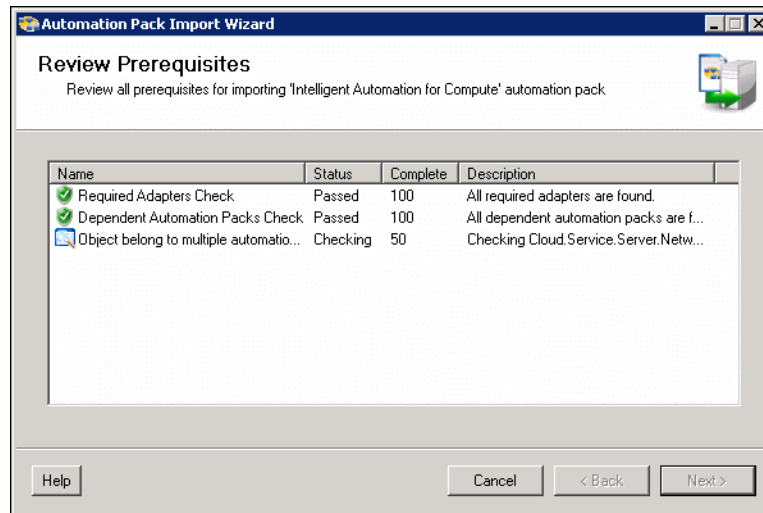
Field	Action
Domain	Enter the name of the domain of the user account used to connect to the Tidal Enterprise Orchestrator Web service target.
User name	Enter the username for the user account associated with target.
Password	Enter the password assigned to the user account.

- Step 11** Click **Next** to continue.

Figure 2-15 Automation Pack Import Wizard—Intelligent Automation for Compute—VMware Keystore Password

Step 12 Enter a password to be used to access the VMware keystore, then click **Next** to continue.

Figure 2-16 *Intelligent Automation for Compute—Review Prerequisites*



The Review Prerequisites panel displays the prerequisites for the automation pack being imported. The green check mark indicates that the prerequisite was found on the computer. If all prerequisites are found, the wizard automatically continues to the Intelligent Automation for Cloud Starter Automation Pack.

A red X indicates that the prerequisite was not found on the computer. When this occurs, the import process is stopped and cannot continue until all prerequisites have been met.

Step 13 Proceed to [Import and Configure the Intelligent Automation for Cloud Starter Automation Pack](#).

Import and Configure the Intelligent Automation for Cloud Starter Automation Pack

The wizard will now guide you through importing the Intelligent Automation for Cloud Starter Automation Pack.



Note

It is recommended that you read through this section prior to importing the automation pack to identify and obtain all the necessary information that needs to be provided in the wizard panels. This will help streamline the import process.

Step 1 On the General Information panel, review the information about the automation pack.

Figure 2-17 Automation Pack Import Wizard—Intelligent Automation for Cloud Starter—General Information

Automation Pack Import Wizard

General Information
General information of 'Intelligent Automation for Cloud Starter' automation pack

Name:
Intelligent Automation for Cloud Starter

Company:
Cisco Systems, Inc.

Version:
3.1.0

Description:
This automation pack contains Orchestrator processes, Portal services and Portal portlets that implement basic IaaS cloud.
Cisco Intelligent Automation for Cloud Starter Edition 3.1 (C) 2012 Cisco Systems, Inc.


Help Cancel < Back Next >

Step 2 Click **Next** to continue.

Figure 2-18 Automation Pack Import Wizard—Intelligent Automation for Cloud Starter—Cloud Portal Integration API Connection

Step 3 On the Cloud Portal Integration API Connection panel, specify for the following information to create a connection to the Cloud Portal:

Field	Action
Host name	Enter the IP address or the server name of the server where Cloud Portal is installed. For example, enter: <servername>.domain.local
Port number	Port number used to connect to the Cloud Portal server. The default port number is 8080 .

Field	Action
User name Password	<p>Enter a username and password for the user account that will be used for the connection to Cloud Portal.</p> <p>This user account is referred to as the <i>nsAPI user account</i>. Later in the configuration process, you will create the actual account in Cloud Portal using the username and password you set here.</p> <p> Caution It is strongly recommended that you record the nsAPI username and password that you create now on the TEO-Cloud Portal Integration API Connection User Account Credentials worksheet in Appendix D “Solution Deployment Worksheets.” You will need this information when you create the nsAPI user account. If the username and password do not match those you have created here, TEO will not be able to communicate with Cloud Portal.</p> <p>Note If you change the nsAPI username and password, you must also edit the extended target properties for <code>Cloud.Configuration.CloudPortal.API.Password</code> and <code>Cloud.Configuration.CloudPortal.API.User</code> with the new username. The steps for editing the extended target properties, <i>see the Cisco Intelligent Automation for Cloud User Guide.</i></p>
Ignore certificate errors	Check or uncheck the check box to indicate whether the target should ignore any certificate errors on the specified web site. If the check box is checked, all errors will be ignored.
Base URL	Enter the URL to the server where Cloud Portal is installed: <code>http://<Hostname>:<Port>/IntegrationServer/services</code>

Step 4 Click **Next** to continue.

Figure 2-19 Automation Pack Import Wizard—Intelligent Automation for Cloud Starter—Cisco Cloud Portal Request Center API Connection

Step 5 On the Cisco Cloud Portal Request Center API Connection panel, specify for the following information for connecting to the Cisco Cloud Portal Request Center API:

Field	Action
Host name	Enter the IP address or the server name of the server where Cisco Cloud Portal Request Center is installed. For example, enter: <servername>.domain.local
Port number	Enter the port number used to connect to the Cisco Cloud Portal Request Center. The default port number is 8080 .
Base URL	Enter the URL to the server where Cloud Portal Request Center is installed: http://<Host name>:<Port number>/RequestCenter
Ignore certificate errors	Check or uncheck the check box to indicate whether the target should ignore any certificate errors on the specified web site. If the check box is checked, all errors will be ignored.
User name Password	Enter the username and password for the nsAPI user account that you created in Step 3 .

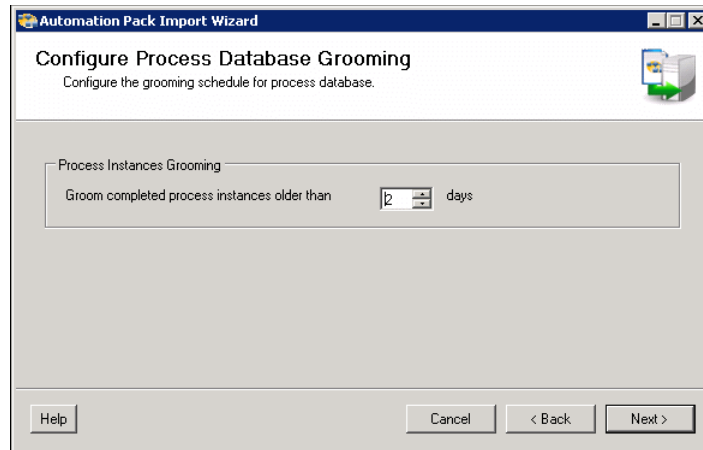
Step 6 Specify the Cisco Service Portal Request Center and Service Link connection information.

Figure 2-20 Automation Pack Import Wizard—Intelligent Automation for Cloud Starter—Cisco Service Portal Server Connection

Field	Description
Server	Enter the IP address or the server name of the server where Cisco Cloud Portal Server is installed. For example, enter: <servername>.domain.local
ServiceLink Port	Enter the port number used to connect to ServiceLink on the Cisco Cloud Portal Server. The default port number is 8080.
RequestCenter Port	Enter the port number used to connect to RequestCenter on the Cisco Cloud Portal Server. The default port number is 8080.
Access Service Portal via secure Socket Layer (SSL)	You can connect to the Cisco Cloud Portal Server using SSL by checking this option and configuring the Cisco Cloud Portal Server to accept SSL Request.
Ignore Secure Socket Layer (SSL) certificate errors	Check this option to ignore SSL certificate errors.
Validate this Connection	You can validate the connection to the Cisco Cloud Portal Server by selecting this option. If this option is selected, the connection and credentials will be verified before continuing the TAP import.
User name	Enter the username for the user account associated with Cisco Cloud Portal Server.
Password	Enter the password assigned to the user account.

Step 7 Click **Next** to continue.

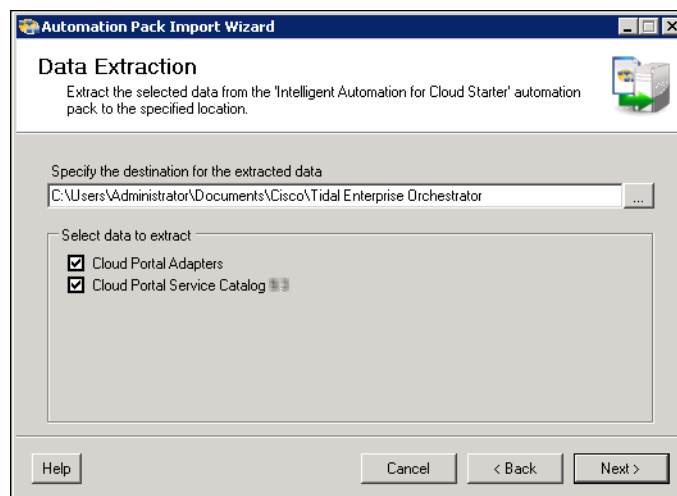
Figure 2-21 Automation Pack Import Wizard—Intelligent Automation for Cloud Starter—Configure Process Database Grooming



Step 8 On Configure Process Database Grooming panel, specify the number of days to keep process instances in the database. After the specified number of days, the process instances will be deleted from the database.

Step 9 Click **Next** to continue.

Figure 2-22 Automation Pack Import Wizard—Intelligent Automation for Cloud Starter—Data Extraction



The Data Extraction panel is used to specify the destination where the data is extracted on the Tidal Enterprise Orchestrator server.



Note If you uncheck the check boxes, the files will not be extracted.


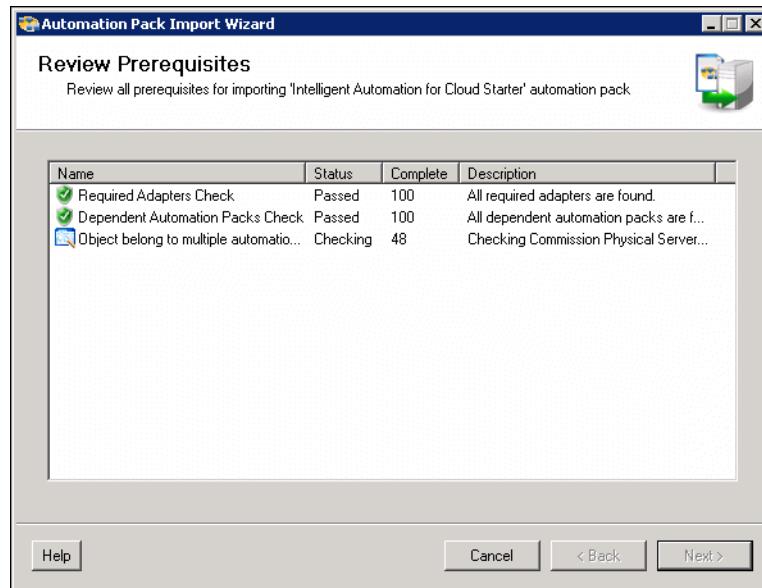
- Step 10** On the Data Extraction panel, accept the default location, or click the **Browse**  tool to specify a different location to extract the files, then click **Next**.

Figure 2-23 Automation Pack Import Wizard—Intelligent Automation for Cloud Starter—Review Prerequisites



The Review Prerequisites panel displays the prerequisites for the automation pack being imported. The green check mark indicates that the prerequisite was found on the computer. If all prerequisites are found, the importing procedures are complete.

A red X indicates that the prerequisite was not found on the computer. When this occurs, the import process is stopped and cannot conclude until all prerequisites have been met.

- Step 11** Proceed to [Import and Configure the Intelligent Automation for Cloud Automation Pack](#).

Import and Configure the Intelligent Automation for Cloud Automation Pack

The wizard will now guide you through importing the Intelligent Automation for Cloud automation pack.

**Note**

It is recommended that you read through this section prior to importing the automation pack to identify and obtain all the necessary information that needs to be provided in the wizard panels. This will help streamline the import process.

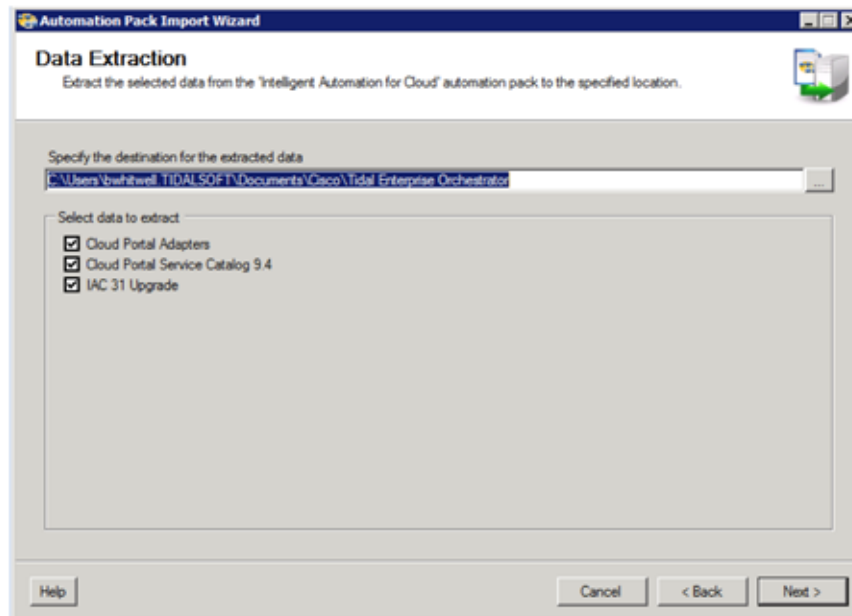
Step 1 On the General Information panel, review the information about the automation pack, then click **Next**.

Figure 2-24 Automation Pack Import Wizard—Intelligent Automation for Cloud—General Information

The screenshot shows a Windows-style dialog box titled "Automation Pack Import Wizard". The main content area is titled "General Information" and contains the following text: "General information of 'Intelligent Automation for Cloud' automation pack". Below this, there are four input fields: "Name:" with the value "Intelligent Automation for Cloud"; "Company:" with the value "Cisco Systems, Inc."; "Version:" which is empty; and "Description:" with the text "This automation pack contains Orchestrator processes and objects for cloud infrastructure orchestration. Cisco Intelligent Automation for Cloud Compute 3.1 (C) 2012 Cisco Systems, Inc.". At the bottom of the dialog, there are four buttons: "Help", "Cancel", "< Back", and "Next >".

Step 2 Enter the destination for the extracted data, and select the data to extract, then click **Next** to continue.

Figure 2-25 Automation Pack Import Wizard—Intelligent Automation for Cloud—Data Extraction



Step 3 The objects will be imported from the Intelligent Automation for Cloud automation pack. After the objects have been imported, review the information on the Completing the Automation Pack Import Wizard panel to verify that it is correct, then click **Close** to close the wizard.

A red X indicates that the prerequisite was not found on the computer. When this occurs, the import process is stopped and cannot conclude until all prerequisites have been met.

Step 4 Proceed to one of the following sections:

- For Linux environments—[Setup for Cloud Portal on Linux](#)
- For Windows environments—[Setup for Tidal Enterprise Orchestrator Server Web Service](#)

Setup for Cloud Portal on Linux



Note

This section pertains only to running Cloud Portal on **Linux** and not Windows. If you are not running CloudPortal on a Linux platform, skip to the next section, [Setup for Tidal Enterprise Orchestrator Server Web Service](#).

If you are running Cloud Portal on a Linux operating system, you must manually configure extended properties for the following targets:

- Cisco Cloud Portal Request Center API
- Cisco Cloud Portal Integration API



Note You must create the Cloud Portal Request Center API target *before* you create the Cisco Cloud Portal Integration API.

For each target, you must manually configure the following extended properties:

- Cloud.Configuration.CloudPortal.IsUnix
- Cloud.Configuration.CloudPortal.UnixTarget

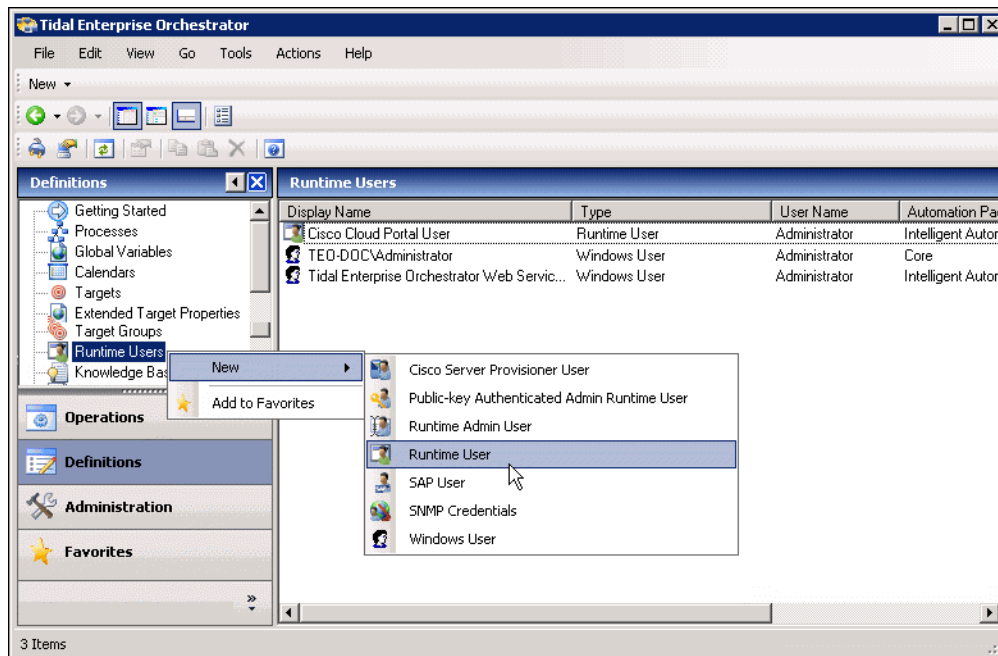
Configure Extended Target Properties for Cisco Cloud Portal Integration API

Before you can configure the extended target properties, for Cisco Cloud Portal Integration API, you must first create a Linux target and a default runtime user for the target.

Create a Runtime User for the Linux Target

- Step 1** In the TEO console, click **Definitions** in the panel on the left to display the Definitions workspace.
- Step 2** Right-click **Runtime Users** in the Definitions panel and choose **New > Runtime User**.

Figure 2-26 Runtime Users View—Add New Runtime User

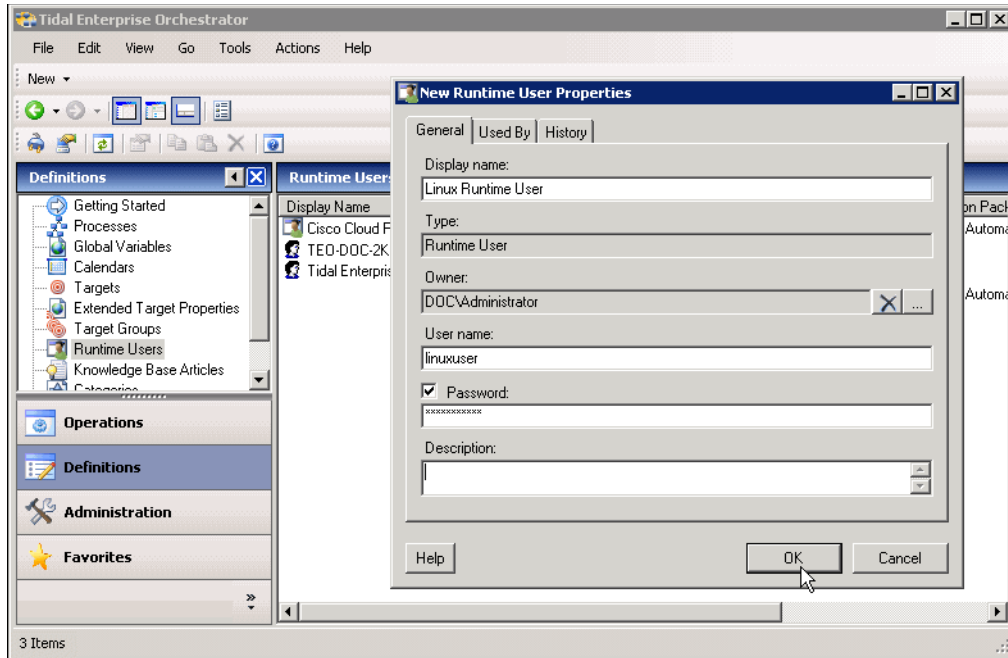


- Step 3** In the New Runtime User Properties dialog box, click the **General** tab, and specify the following information:

Field	Action
Display name	Enter a descriptive display name for the new runtime user.

User name	Enter the user name for the new runtime user. The user must have write access to the on the Linux server drop-box location.
Password	Check the Password check box, then enter the password.
Description	<i>Optional.</i> Enter a description of the runtime user.

Figure 2-27 Runtime Users View—New Runtime User Dialog Box




Step 4 Click **OK**, then proceed to [Create a Target for the Linux Server](#).

Create a Target for the Linux Server

- Step 1 In the Definitions workspace, right-click **Targets** and choose **New > Unix/Linux System**.
- Step 2 In the New Unix/Linux System Properties dialog box, click the **General** tab, then enter a descriptive display name.



Note The **Required Value**  icon displayed on a tab or beside a field indicates that the field is required and is missing a value.

- Step 3 Click the **Connection** tab.
- Step 4 Enter the fully qualified host name for the Linux target.
- Step 5 Uncheck the **Prompt prefix** check box.
- Step 6 From the Default runtime user drop-down list, choose the runtime user you created in the previous section, [Create a Runtime User for the Linux Target](#).

- Step 7 Click the **Advanced** tab.
 - Step 8 From the Use patterns common for the following device drop-down list, choose the Linux target you have just created, then click **OK**.
 - Step 9 Proceed to [Configure the Extended Target Properties for Both Cloud Portal Web Service Targets](#).
-

Configure the Extended Target Properties for Both Cloud Portal Web Service Targets

- Step 1 In the Definitions workspace in the TEO console, click **Targets**.
 - Step 2 Right-click **Cisco Cloud Portal Integration API** in the list and choose **Properties**.
 - Step 3 In the Properties dialog box, click the **Extended Properties** tab.
 - Step 4 In the Extended target properties pane, select **Cloud.Configuration.CloudPortal.IsUnix**, then click **Edit**.
 - Step 5 In the Target Property Value dialog box, choose **true** from the Value drop-down list, then click **OK**.
 - Step 6 Select **Cloud.Configuration.CloudPortal.UnixTarget**, then click **Edit**.
 - Step 7 On the Target Property Value dialog box, click the **Browse** tool next to the Value field to open the Select Target dialog box.
 - Step 8 In the Select Target dialog box, select the Linux target that you created in [Create a Target for the Linux Server, page 2-24](#), then click **OK**.
 - Step 9 Proceed to [Configure Extended Target Properties for Cisco Cloud Portal Request Center API](#).
-

Configure Extended Target Properties for Cisco Cloud Portal Request Center API

- Step 1 In the Definitions workspace in the TEO console, click **Targets**.
 - Step 2 Right-click **Cisco Cloud Portal Request Center API** in the list and choose **Properties**.
 - Step 3 In the Properties dialog box, click the **Extended Properties** tab.
 - Step 4 In the Extended target properties pane, select **Cloud.Configuration.CloudPortal.IsUnix**, then click **Edit**.
 - Step 5 In the Target Property Value dialog box, choose **true** from the Value drop-down list, then click **OK**.
 - Step 6 In the Properties dialog box, select **Cloud.Configuration.CloudPortal.UnixTarget**, then click **Edit**.
 - Step 7 Click the **Browse** tool next to the Value field to open the Select Target dialog box.
 - Step 8 In the Select Target dialog box, select the Linux target that you created in [Create a Target for the Linux Server, page 2-24](#), then click **OK**.
 - Step 9 Proceed to [Setup for Tidal Enterprise Orchestrator Server Web Service](#).
-

Setup for Tidal Enterprise Orchestrator Server Web Service

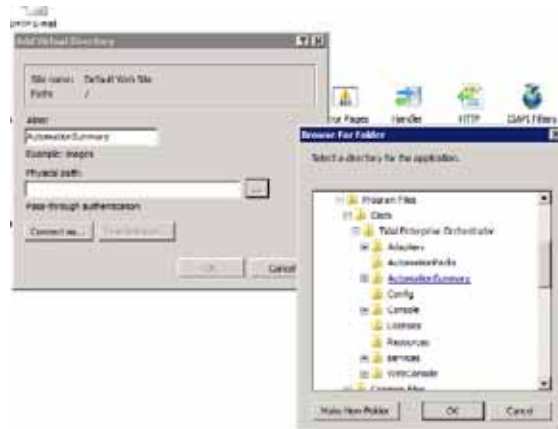
After installing the automation packs, you must:

- Set up the Internet Information Services (IIS) so that AutomationSummary links will work in the ERS portlet.
- Refresh the TEO Server web service. This action allows all of the installed processes to be initialized in TEO web service.

Setup for Internet Information Services

- Step 1 Open Server Manager, then choose **Roles > Web Server(IIS) > Internet Information Services (IIS) Manager**.
- Step 2 Expand *Sites*, right-click on **Default Web Site**, and select **Add Virtual Directory**.
- Step 3 Enter the following information:
 - In the **Alias** text box, enter **AutomationSummary**.
 - In the **Physical Path** text box, browse to and select the folder that contains the Automation Summaries. If you selected the default option when importing the TEO Core Adapter, the path will be:
C:\Program Files\Cisco\Tidal Enterprise Orchestrator\AutomationSummary

Figure 2-28 IIS Setup - Add Virtual Directory

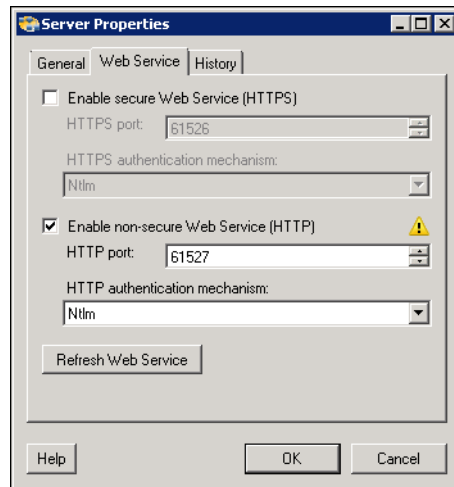


- Step 4 Click **OK**.
- Step 5 Make sure permissions are set appropriately on the folder you selected.
- Step 6 Proceed to [Refresh Server Web Service](#).

Refresh Server Web Service

- Step 1** In the TEO console, click **File > Server Properties** to open the Server Properties dialog box.
- Step 2** Click the **Web Service** tab.

Figure 2-29 Server Properties Dialog Box—Web Service Tab



- Step 3** Click **Refresh Web Service**, then click **OK**.

After you have completed setting up TEO, proceed to one of the following chapters:

- [Chapter 3, “Installing the REX Adapter”](#)—If you do not already have the required REX adapter installed, follow the instructions in this chapter.
- [Chapter 4, “Configuring Cisco Cloud Portal and Deploying Cisco Intelligent Automation for Cloud Content”](#)—If you already have the REX adapter installed, proceed to this chapter to begin configuring Cisco IAC.



CHAPTER 3

Installing the REX Adapter



Note

If you already have the REX adapter installed, skip to [Chapter 4, “Configuring Cisco Cloud Portal and Deploying Cisco Intelligent Automation for Cloud Content.”](#)

This chapter guides you through installing the REX adapter.



Note

You cannot install the REX adapter without first importing the Automation Packs into Tidal Enterprise Orchestrator as directed in [Chapter 2, “Configuring Cisco Tidal Enterprise Orchestrator and Deploying Cisco Intelligent Automation for Cloud Content.”](#) The files required for installing the REX adapter are shipped with the Intelligent Automation for Cloud Starter automation pack and can only be unpacked when the automation pack is imported.

Prerequisites

Before you install the REX adapter, you **must** meet the following requirements:

- You have carefully reviewed [Chapter 1, “Solution Prerequisites.”](#) for Cloud Portal, Cloud Portal database, and other Cisco IAC requirements.
- You have installed Cloud Portal (for the correct version, see the [Cisco Intelligent Automation for Cloud Compatibility Matrix](#). For installation instructions, see the [Cloud Portal Installation Guide](#) for the respective Cloud Portal version.
- You have imported and configured the Cisco IAC automation packs in TEO. The files required for installing the REX adapter included in the Intelligent Automation for Cloud Starter Automation Pack. For instructions, see [Chapter 2, “Configuring Cisco Tidal Enterprise Orchestrator and Deploying Cisco Intelligent Automation for Cloud Content.”](#)

Apply the Cloud Portal Patch

Before you install the REX adapter, you must first apply the Cloud Portal patch.

Step 1 Download and extract the patch file, which includes a Readme file.



Note To find the patch for this release, see the [Cisco Intelligent Automation for Cloud Compatibility Matrix](#).



Note The package name is the same for both Windows and Linux.

Step 2 Follow the instructions for applying the hotfix in the Readme. The instructions provide important steps for copying extracted files to different deployed directories.

Step 3 Proceed to [Install the REX Adapter](#).

Install the REX Adapter

After installing Cisco Service Portal and before performing the Cisco IAC configurations covered in this guide, you must install the REX adapter.

When the Intelligent Automation for Cloud Starter Automation Pack is imported in TEO (see [Import and Configure the Intelligent Automation for Cloud Starter Automation Pack, page 2-14](#)), the REX adapter installation package (**rexAdapter_<release_number>.zip**) is placed by default in the following location on the Tidal Enterprise Orchestrator server:

```
<My Documents>/Cisco/Tidal Enterprise Orchestrator/Extracted Data/Cloud Portal
Adapters/rexAdapter
```

Step 1 Extract **rexAdapter_<release_number>.zip** from its default location on the TEO server to a temporary location (hereafter referred to as <rex>).

- Step 2** Copy `<rex>/adapters/adapter_rex.jar` to the deployed `<JBOSS_DIR>/standalone/deployments/ServiceLink.war/WEB-INF/lib` directory.
- Step 3** Extract `adk.zip`, which is located in the unzipped Patch directory for this release. The extraction creates the `<adk>` folder.
- Step 4** Open a command window, and cd to the `<adk>` folder.
- Step 5** Run the following command:
- Windows: `adapter_dbinstaller.cmd`
 - Linux: `adapter_dbinstaller.sh`

The following is a sample run for each database:

Database	Sample Run
SQL Server	<pre>c:\adk>adapter_dbinstaller.cmd found bin\java.exe Please enter the database connection information. Database Type [SQLSERVER]: Database Hostname [localhost]: Database Port [1433]: Database Name [RequestCenter]: Username [RCUSER]: RCUser Password: Testing database connection: Success! Adapter Deployment Descriptor File: c:\rex\deploy\rex.xml</pre>
Oracle	<pre>c:\adk>adapter_dbinstaller.cmd found bin\java.exe Please enter the database connection information. Database Type [SQLSERVER]: ORACLE Database Hostname [localhost]: Database Port [1521]: Oracle SID [ORCL]: Username [RCUSER]: RCUser Password: Testing database connection: Success! Adapter Deployment Descriptor File: c:\rex\deploy\rex.xml</pre>

- Step 6** Stop the JBoss application server.



Note For instructions, see “How to Stop/Start the JBoss Server” in the [Cloud Portal Installation Guide](#) for the respective Cloud Portal version.

- Step 7** Delete the contents in the following directory:

`<JBOSS_DIR>\standalone\tmp\work`

- Step 8** Restart the JBoss application server.



Note For instructions, see “How to Stop/Start the JBoss Server” in the [Cloud Portal Installation Guide](#) for the respective Cloud Portal version.

Step 9 Proceed to [Chapter 4, “Configuring Cisco Cloud Portal and Deploying Cisco Intelligent Automation for Cloud Content.”](#)



CHAPTER 4

Configuring Cisco Cloud Portal and Deploying Cisco Intelligent Automation for Cloud Content



Note

Before you can complete the tasks in this chapter, you **MUST** complete **all** of the tasks, in sequence, that are presented in the previous chapters. You cannot proceed unless you have installed the REX adapter and performed necessary initial configurations for Cisco Cloud Portal.

This chapter walks you through importing, deploying, and configuring important components of Cisco Intelligent Automation for Cloud—catalogs, portals, and agents. It includes the following sections:

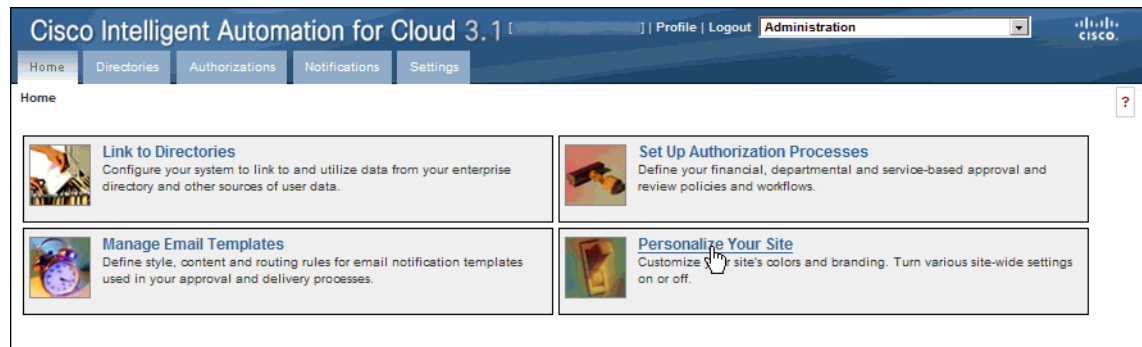
- [Enable Web Services](#)
- [Create a Dropbox for Data Synchronization](#)
- [Import and Deploy Intelligent Automation for Cloud Service Catalogs](#)
- [Import and Deploy Portal Packages](#)
- [Modify Maximum Numbers for Tabs, Portals, and Portlets](#)
- [Modify Column Settings for the Site Homepage](#)
- [Set Permissions for Portals and Portlets](#)
- [Adding the Approvals Portlet to the My Approvals Portal Page](#)
- [Adding the OrderStatus Portlet to the My Orders Portal Page](#)
- [Adding Portal Pages to My Workspace](#)
- [Assign Additional Permissions for the Cloud Provider Technical Administrator Role](#)
- [Assign Additional Permissions for the Organization Technical Administrator Role](#)
- [Assign Additional Permissions for the Server Owner Roles](#)

Enable Web Services

When you imported the Intelligent Automation for Compute automation pack (page 2-9) into Tidal Enterprise Orchestrator (TEO), you enabled web services and specified HTTP port and authentication. You must also enable web services in Cloud Portal (CP) to enable a bidirectional communication path between TEO and CP.

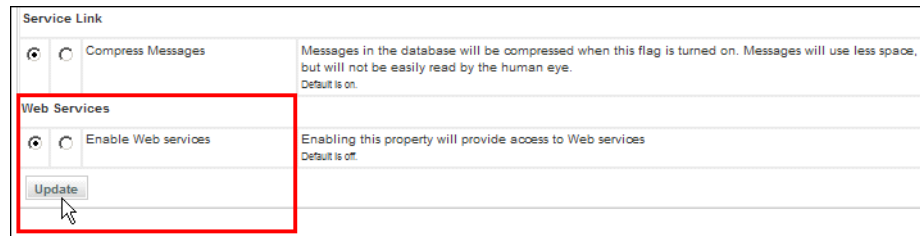
- Step 1** On the Cloud Portal Home page, choose **Administration** from the module drop-down list.
- Step 2** On the Administration Home page, click **Personalize Your Site**.

Figure 4-1 Administration Home Page—Personalize Your Site



- Step 3** On the Customizations page, scroll down to the bottom of the page, and click the **On** radio button for the Enable Web services setting. Click **Update** immediately under the Web services setting.

Figure 4-2 Customizations—Enabling Web Services



- Step 4** Proceed to [Create a Dropbox for Data Synchronization](#).

Create a Dropbox for Data Synchronization

The dropbox location must be shared between the Cisco Cloud Portal (CP) and the Tidal Enterprise Orchestrator (TEO) servers. While there are several ways to configure this, whether using directory integration or not and whether the dropbox location is local to or remote from the CP and PO servers, the nsAPI user account in CP and the Runtime User account in TEO must have read / write access to the dropbox.

**Tip**

Recommendation: The nsAPI user account in CP and Runtime User account in TEO should be the same.

**Note**

Linux users: Configure the extended properties **Cloud.Configuration.CloudPortal.IsUnix** and **Cloud.Configuration.CloudPortal.UnixTarget**. If you have not yet completed the tasks involved, see [Setup for Cloud Portal on Linux, page 2-22](#), then return to this chapter to continue.

Create a dropbox that Cloud Portal and Tidal Enterprise Orchestrator (TEO) will use to exchange information.

Step 1 Create the dropbox folder:

- Windows: Create a folder called **c:\dropbox** on the Cloud Portal server, then share it with TEO.
- Linux: Create a folder called **C:\dropbox** on the Cloud Portal server. TEO will access the dropbox for data synchronization via SFTP.

Ensure the dropbox folder is read/write accessible for everyone.

Step 2 In the dropbox folder, create three subfolders using the following suggested names:

- input
- backup
- temp

Step 3 Proceed to [Import and Deploy Intelligent Automation for Cloud Service Catalogs](#).

Import and Deploy Intelligent Automation for Cloud Service Catalogs

**Note**

The REX adapter **must** be installed on the Cloud Portal server before you import and deploy the service catalogs. If you have not installed the REX adapter, see [Chapter 3, “Installing the REX Adapter,”](#)

The Cisco IAC service catalog and portal content is included in files that are extracted when the Cisco Intelligent Automation for Cloud automation pack is imported. These files must be imported and deployed in Cloud Portal.

In this section, you will complete the following tasks in sequence:

- Copy Service Catalog Files to Cloud Portal Server

- Import and Deploy Service Catalogs

Copy Service Catalog Files to Cloud Portal Server

The Cisco IAC service catalog files that are extracted when the Cisco Intelligent Automation for Cloud automation pack is imported must be copied from the Tidal Enterprise Orchestrator server to the Cloud Portal server to facilitate importing and deploying Cisco IAC in Cloud Portal.

-
- Step 1** On the Tidal Enterprise Orchestrator server, navigate to the location where the files were extracted during the automation pack import process. By default, the files are copied to the following location on the server:
- ```
C:\Users\\Documents\Cisco\Tidal Enterprise Orchestrator\Extracted Data\Cisco Cloud Portal Service Catalog 9.4
```
- Step 2** Copy the following files to a folder on the Cloud Portal server:
- CP\_Common\_3-1.xml
  - CP\_Services\_3-1.xml
  - CP\_Transport\_Package\_3-1.xml
- Step 3** Proceed to [Import and Deploy Service Catalogs](#).
- 

## Import and Deploy Service Catalogs

Complete the following procedure to import and deploy catalogs in Cloud Portal.



### Note

You must be logged into Cloud Portal with administrator privileges to perform the procedures in this chapter.

---

- 
- Step 1** Open Cloud Portal in your browser and log in with administrator privileges.
- Step 2** Choose **Catalog Deployer** from the module drop-down list.
- Step 3** In the Deployment Packages pane, and choose **Action > Import** from the drop-down list.
- Step 4** On the Import Package from File dialog box, click **Browse** to navigate to the folder where you saved the service catalog files. (See [Step 2 in Copy Service Catalog Files to Cloud Portal Server, page 4-4](#).)
- Step 5** Select the **CP\_Common\_3-1.xml** file and click **Import**.
- Step 6** On the Package Import dialog box, when the message *Package Imported Successfully* displays, click **OK**. The Deployment Packages window refreshes to display the imported package in the Received for Deployment view.
- Step 7** Repeat [Step 3](#) through [Step 6](#) to import the all of the remaining catalog files.
- Step 8** In the Deployment Packages pane, choose **Action > Deploy Multiple Packages** from the drop-down list.
- Step 9** On the Batch Deployment tab, click **Add Packages**.
- Step 10** On the Select Packages dialog box, check the check boxes of the packages you need to import, then click **Select**.

- Step 11** On the Batch Deployment tab, check the **Selected Items** check box and ensure that all check boxes in the folder are checked (Figure 4-2 on page 4-5).
- Step 12** Click **Deploy**.
- Step 13** When each package displays *Succeeded* next to it, click **Done**.
- Step 14** Proceed to [Import and Deploy Portal Packages](#).
- 

## Import and Deploy Portal Packages

Cisco IAC ships with packaged stylesheets, image files, portals, and portlets to provide an easy-to-use portal for ordering services. This section guides you through deploying Cisco IAC content in Cloud Portal.

In this section, you will complete the following tasks in sequence:

- Copy the Cisco IAC Portlets package and extract files
- Configure Cloud Portal Stylesheets
- Import Portal Pages

## Copy the Cisco IAC Portlets Package and Extract Files

The Cisco Intelligent Automation for Cloud automation pack includes the Cisco IAC Portlets package (IACPortlets\_<release\_number>), which was extracted to the Tidal Enterprise Orchestrator server when you imported the automation pack. (See [Import and Configure the Intelligent Automation for Compute Automation Pack, page 2-9](#).) This package contains the files you need to deploy portlets, JavaScripts, images, and stylesheets to Cloud Portal.

- Step 1** On the Tidal Enterprise Orchestrator server, navigate to the following folder where IACPortlets\_<release\_number> was extracted. The package is extracted by default to the following directory:

```
C:\Users\<username>\Documents\Cisco\Tidal Enterprise Orchestrator\Extracted Data
```

- Step 2** Extract **IACPortlets\_<release\_number>** to a temporary location. It will create an IACPortlets\_<release\_number> folder.

- Step 3** Stop the JBoss application server.



**Note** For instructions, see “How to Stop/Start the JBoss Server” in the [Cisco Service Portal 9.4 Installation Guide](#).

---

- Step 4** In the IACPortlets\_<release\_number> folder, locate RequestCenter\_war.zip, then extract it to the following directory:

```
<JBOSS_DIR>\standalone\deployments\RequestCenter.war
```

Step 5 Restart the JBoss application server.



**Note** For instructions, *see* “How to Stop/Start the JBoss Server” in the [Cisco Service Portal 9.4 Installation Guide](#).

Step 6 Proceed to [Configure Cloud Portal Stylesheets](#).

## Configure Cloud Portal Stylesheets

You must now configure Cloud Portal to use the stylesheets that are packaged with Cisco IAC. Complete the following steps to configure the stylesheets in Cloud Portal.

- Step 1 Open Cloud Portal in your browser and log in to the application.
- Step 2 On the Cloud Portal Home page, choose **Administration** from the module drop-down list.
- Step 3 On the Administration Home page, click **Personalize Your Site** ([Figure 4-1 on page 4-2](#)).
- Step 4 On the Customizations page, scroll down the common settings pane (about halfway down the page) and click the **On** radio button for the Enable Custom Style Sheets setting.

**Figure 4-3** Customizations—Enabling Custom Style Sheets

| On                               | Off                              | Setting                         | Description                                                                                                                                        |
|----------------------------------|----------------------------------|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Common</b>                    |                                  |                                 |                                                                                                                                                    |
| <input type="radio"/>            | <input checked="" type="radio"/> | Enable Custom Header Footer     | Site will add content from the custom header and footer HTML.<br>Default is off.                                                                   |
| <input checked="" type="radio"/> | <input type="radio"/>            | Enable Custom Style Sheets      | Site will utilize the custom stylesheet allowing for the changing of logos, color schemes, fonts and others.<br>Default is off.                    |
| <input type="radio"/>            | <input checked="" type="radio"/> | Directory Integration           | Enable the Directories feature that searches for and imports users into the site from an external datasource (e.g. LDAP).<br>Default is off.       |
| <input type="radio"/>            | <input checked="" type="radio"/> | Restrict Site Administrator URL | Allow only those users with the Site Administrator Role to log in using the administrator URL (i.e., bypassing Single Sign-On).<br>Default is off. |
| <input checked="" type="radio"/> | <input type="radio"/>            | Remember Password Enabled       | Enable or disable Remember Me functionality on the login page.<br>Default is on.                                                                   |

- Step 5 Click **Update** at the *bottom* of the page to save the settings.
- Step 6 Click **Custom Styles** in the right menu.



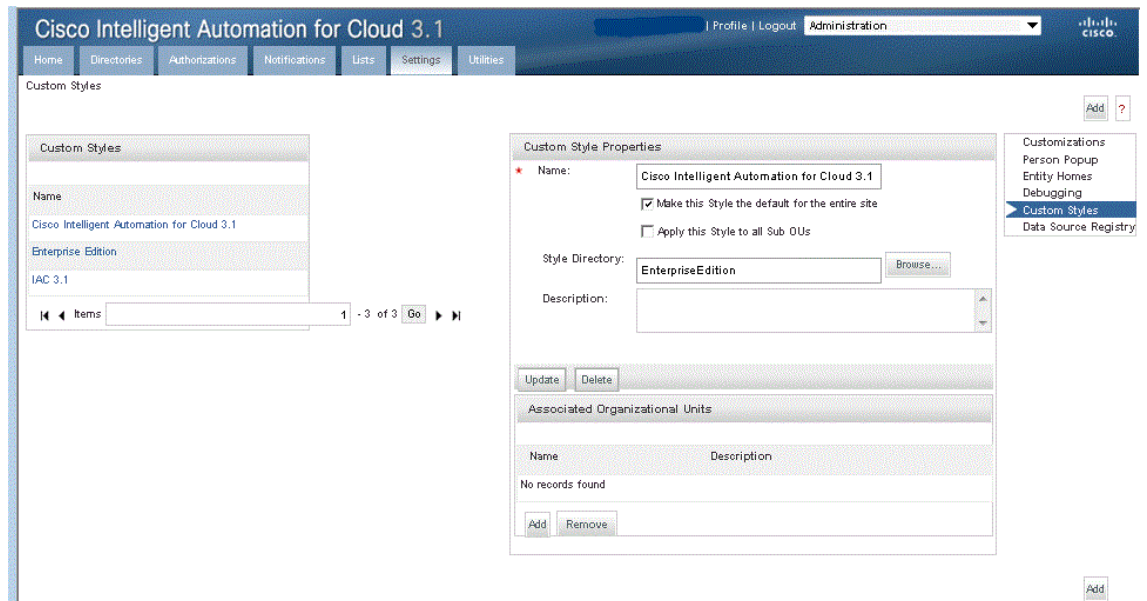
Figure 4-4 Custom Styles



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

- Step 7** Click **Add** to open the Custom Style Properties window.
- Step 8** In the Name field, enter **Cisco Intelligent Automation for Cloud 3.1**.
- Step 9** Check the **Make this Style the default for the entire site** check box.
- Step 10** In the Style Directory field, click **Browse**.
- Step 11** Click the **EnterpriseEdition** radio button, then click **OK**.
- Step 12** On the Custom Style Properties window, click **Create** to add the custom style.

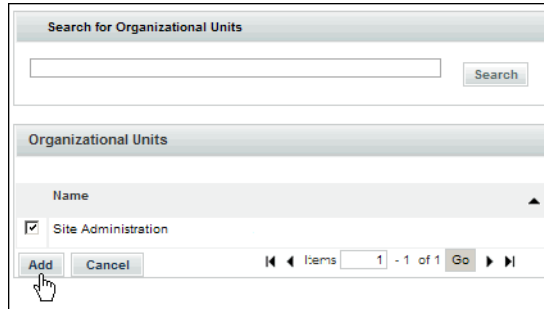
Figure 4-5 Custom Style Properties—Associated Organization Units



- Step 13** On the Custom Style Properties page, navigate to the Associated Organizational Units area.
- Step 14** Click **Add** to open the Search for Organizational Units dialog box.

- Step 15** Click **Search** to browse for the organizational units to which to associate the custom style properties. You can use the wildcard \* to search for all organizational units or to narrow the search results.

**Figure 4-6** Search for Organizational Units



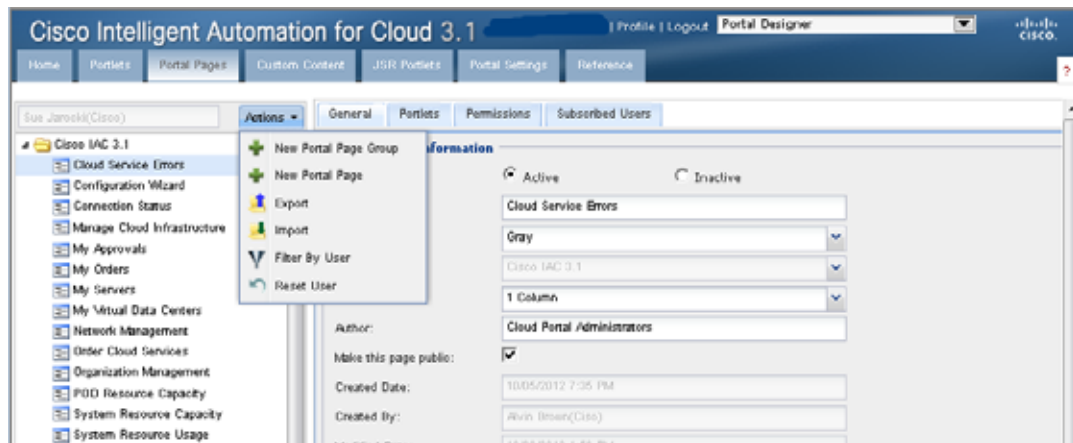
- Step 16** Check the **Site Administration** check box, then click **Add**.
- Step 17** Proceed to [Import and Deploy Portal Pages](#).

## Import and Deploy Portal Pages

Deploy the Cisco IAC portal page content by importing it from the All\_Portal\_Pages.xml portal page file, located in the IACPortlets folder.

- Step 1** Choose **Portal Designer** from the module drop-down list to open Portal Designer.
- Step 2** In Portal Designer, click the **Portal Pages** tab.
- Step 3** In the left navigation pane, click **Actions** and choose **Import** from the drop-down list.

**Figure 4-7** Portal Designer—Import Portal Pages Menu



- Step 4** On the Import Portal Pages dialog box, click the **Overwrite** radio button in the Conflict Resolution field.

- Step 5** In the Import from File field, click **Browse** to navigate to the IACPortlets folder that you extracted in [Copy the Cisco IAC Portlets Package and Extract Files, page 4-5](#).
- On the Choose File to Upload dialog box, select the **All\_Portal\_Pages.xml** file and click **Open**.
  - On the Import Portal Pages dialog box, click **Import**.
  - Close the Import Complete dialog box.
- Step 6** Refresh your browser to view the imported portal.
- Step 7** Proceed to [Modify Maximum Numbers for Tabs, Portals, and Portlets](#).

## Modify Maximum Numbers for Tabs, Portals, and Portlets

The portals and portlets that you imported and deployed will be accessible in the My Workspace module in the form of tabs. Before you add tabs in My Workspace for portal access, you must first modify the maximum number of tabs, portals, and portlets that can be displayed.

- Step 1** Choose **Portal Designer** from the module drop-down list, then click the **Portal Settings** tab.
- Step 2** On the Portal Settings tab, click the cell in the Value column for each of the following settings, and enter the following values for each field (see [Figure 4-8 on page 4-10](#)):

| Field                                             | Value |
|---------------------------------------------------|-------|
| Maximum Number of Tabs in Portal                  | 10    |
| Maximum Number of Portlets on a Tab               | 6     |
| Maximum Number of Grid Portlets on a Tab          | 6     |
| Maximum Number of Private Portal Pages in Portal  | 2     |
| nsAPI Page Size For Transactional Data            | 20    |
| nsAPI Page Size For Directory Data                | 20    |
| nsAPI Page Size For ServiceItem and Standard Data | 20    |
| nsAPI Page Size For Defined and Custom Data       | 20    |

Figure 4-8 Portal Designer—Modify Maximum Numbers of Tabs, Portal Pages, and Portlets

The screenshot shows the 'Portal Designer' interface with the 'Portal Settings' tab selected. The 'General' section contains a table of settings. The following table represents the data visible in the screenshot:

| Setting                                           | Value | Description                                                                                                                                                                                                         |
|---------------------------------------------------|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maximum Number of Tabs in Portal                  | 10    | The maximum number of portal pages allowed for display in the Service Portal. Default = 6                                                                                                                           |
| Maximum Number of Portlets on a Tab               | 6     | The maximum number of portlets allowed to be included on a portal page. Default = 6                                                                                                                                 |
| Maximum Number of Grid Portlets on a Tab          | 6     | The maximum number of grid portlets allowed to be included on a portal page. Default = 4                                                                                                                            |
| Maximum Number of Private Portal Pages in Portal  | 2     | The maximum number of private pages an end user can maintain in Service Portal. Default = 2                                                                                                                         |
| nsAPI Page Size For Transactional Data            | 20    | Default number of records returned by nsAPI and/or Portlets when the page limit is not specified. (Note: This setting is applicable to Requisitions, Requisition Entries, Authorizations, and Tasks.)               |
| nsAPI Page Size For Directory Data                | 20    | Default number of records returned by nsAPI and/or Portlets when the page limit is not specified. (Note: This settings is applicable for Peoples, OUs, Groups and Accounts.)                                        |
| nsAPI Page Size For ServiceItem And Standard Data | 20    | Default number of records returned by nsAPI and/or portlets when the page limit is not specified. (Note: This setting is applicable for Standards, Service Items and All Service Items.)                            |
| nsAPI Page Size For Defined And Custom Data       | 20    | Default number of records returned by nsAPI and/or Portlets when the page limit is not specified. (Note: This setting is applicable for Categories, Services, Offerings, Agents, Agreements, Userdefined Contents.) |

Below the table, there is an 'Update' button.

**Step 3** Click **Update**, then proceed to [Modify Column Settings for the Site Homepage](#).

# Modify Column Settings for the Site Homepage

The columns setting for Site Homepage must be set to 1. Check the column settings and modify, if necessary.

- Step 1** In Portal Designer, click the **Portal Pages** tab.
- Step 2** In the left navigation pane, expand the **System** folder and select the **Site Homepage** portal.

**Figure 4-9** Portal Page Layout Setting

The screenshot shows the configuration interface for the 'Site Homepage' portal. The 'Portal Page Information' section includes fields for Name, Theme, Page Group, Layout, Author, and Description. The 'Layout' dropdown menu is open, showing options: 1 Column, 2 Columns, 3 Columns, 1-2 Columns, 1-2-1 Columns, and 2-2 Columns. The 'Layout Configuration' table below shows the current settings for the layout.

| Name                     | Value |
|--------------------------|-------|
| Section 0 Column 0 Width | 1     |
| Portlet Borders          | false |
| Portlet Headers          | false |

- Step 3** In the Portal Page Information pane, locate the Layout drop-down list. If the Layout is not set to **1 Column**, choose **1 Column**.
- Step 4** Click **Save**, then proceed to [Set Permissions for Portals and Portlets](#).

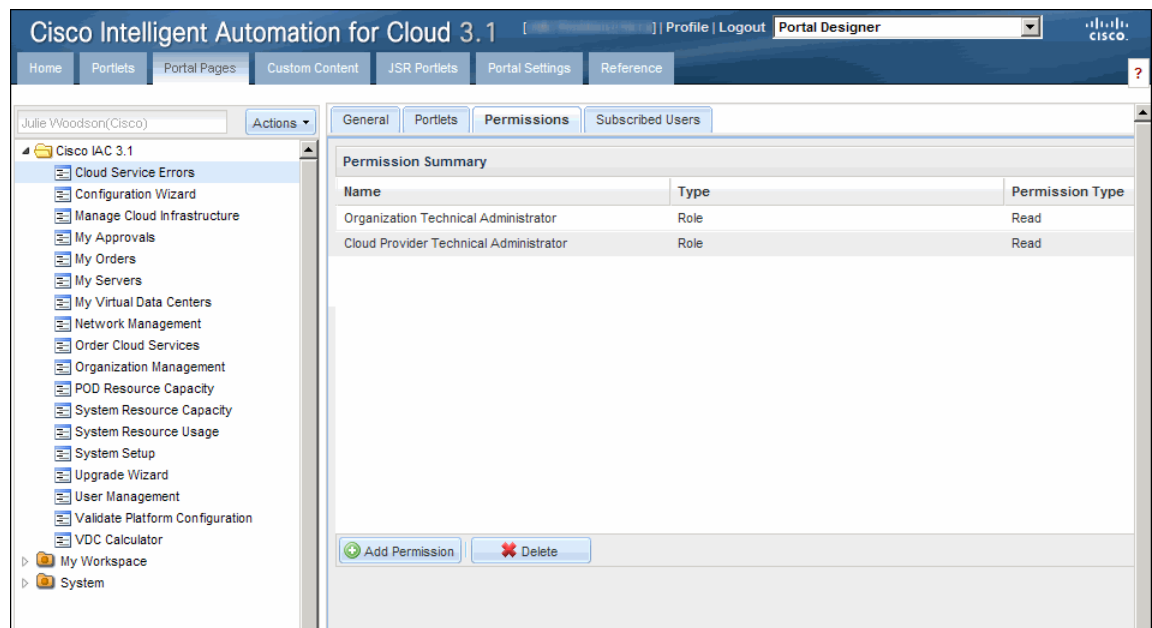
## Set Permissions for Portals and Portlets

After you import the portals, you must add *read-only* permissions for the portals using the Portal Designer.

### Set Permissions for the MyWorkspace Portal Pages

- Step 1 In Portal Designer, click the **Portal Pages** tab.
- Step 2 In the left navigation pane, expand the Cisco IAC folder, choose one of the portal pages. then click the **Permissions** tab.

Figure 4-10 Portal Designer—Portal Page Permissions



**Step 3** Click **Add Permission** to expand the Add Permission area of the page.

**Figure 4-11** Portal Designer—Add Permission to Portal Page

**Step 4** From the Object Type drop-down list, choose **Role**, then click **Search** to display a list of user roles.

**Step 5** Select **Cloud Provider Technical Administrator**.

**Step 6** Click **Add Permissions**.

**Step 7** From the Permissions To drop-down list, choose **Read Only**, then click **Add**.

**Step 8** Repeat [Step 2](#) through [Step 7](#) for the remaining portals in the Cisco IAC folder, setting **read/write** role permissions as shown in the following table.

| Portal                      | User Role (Read Only)                                                                                                                       |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Configuration Wizard        | Cloud Provider Technical Administrator                                                                                                      |
| Connection Status           | Cloud Provider Technical Administrator                                                                                                      |
| Cloud Service Errors        | Cloud Provider Technical Administrator                                                                                                      |
| Manage Cloud Infrastructure | Cloud Provider Technical Administrator                                                                                                      |
| My Approvals                | Cloud Provider Technical Administrator<br>Organization Technical Administrator                                                              |
| My Orders                   | Cloud Provider Technical Administrator<br>Organization Technical Administrator<br>Virtual and Physical Server Owner<br>Virtual Server Owner |
| My Servers                  | Cloud Provider Technical Administrator<br>Organization Technical Administrator<br>Virtual and Physical Server Owner<br>Virtual Server Owner |
| My Virtual Data Centers     | Cloud Provider Technical Administrator<br>Organization Technical Administrator<br>Virtual and Physical Server Owner<br>Virtual Server Owner |
| Network Management          | Cloud Provider Technical Administrator                                                                                                      |
| Order Cloud Services        | Cloud Provider Technical Administrator<br>Organization Technical Administrator<br>Virtual and Physical Server Owner<br>Virtual Server Owner |

| Portal                   | User Role (Read Only)                                                                                                                       |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Organization Management  | Cloud Provider Technical Administrator<br>Organization Technical Administrator                                                              |
| POD Resource Capacity    | Cloud Provider Technical Administrator                                                                                                      |
| Site Homepage            | Cloud Provider Technical Administrator<br>Organization Technical Administrator<br>Virtual and Physical Server Owner<br>Virtual Server Owner |
| System Resource Capacity | Cloud Provider Technical Administrator                                                                                                      |
| System Resource Usage    | Cloud Provider Technical Administrator<br>Organization Technical Administrator<br>Virtual and Physical Server Owner<br>Virtual Server Owner |
| System Setup             | Cloud Provider Technical Administrator                                                                                                      |
| Upgrade Wizard           | Cloud Provider Technical Administrator                                                                                                      |
| User Management          | Cloud Provider Technical Administrator<br>Organization Technical Administrator                                                              |
| VDC Calculator           | Cloud Provider Technical Administrator                                                                                                      |

**Step 9** Proceed to [Set Permissions for Portlets](#).

## Set Permissions for Portlets

Set permissions for user roles for all of the portlets that you have imported. Permissions for all portlets for the Site Homepage must be set to *read-only*; only the Admin (person) should have *read/write* permissions.

- 
- Step 1** In Portal Designer, click the **Portlets** tab.
- Step 2** Set *read-only* permissions for the Site Homepage:
- In the left navigation pane, expand the **HTML** folder, click **Homepage\_Welcome**, then click the **Permissions** tab.
  - Click **Add Permission** to expand the Add Permission area of the page ([Figure 4-11 on page 4-13](#)).
  - From the Object Type drop-down list, choose **Role**, then click **Search** to display a list of the roles that are available.
  - In the Role list, press and hold **Ctrl**, and click the following roles:
    - Cloud Provider Technical Administrator
    - Organization Technical Administrator
    - Virtual Server Owner
    - Virtual and Physical Server Owner
  - From the Permission To drop-down list, choose **Read**, then click **Add**.



- Step 3** Set read permissions for the remaining portlets:
- In the **HTML** folder in the left navigation pane, click a portlet, then click the **Permissions** tab.
  - Click **Add Permission** to expand the Add Permission area of the page.
  - From the Object Type drop-down list, choose **Role**, then click **Search** to display a list of the roles that are available.
  - In the Role list, press and hold **Ctrl**, and click the following roles:
    - Cloud Provider Technical Administrator
    - Organization Technical Administrator
  - From the Permissions To drop-down list, choose **Read Only**, then click **Add**.
  - Repeat [Step 3a.](#) through [Step 3e.](#) for the following portlets, setting permissions for the user roles indicated in the following table:

**Table 4-1** Portlet Permissions

| Portlet                    | User Role (Read Only)                                                                                                                       |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>HTML folder:</b>        |                                                                                                                                             |
| CloudAdmin_OrgManagement   | Cloud Provider Technical Administrator<br>Organization Technical Administrator                                                              |
| CloudAdmin_SystemSetup     | Cloud Provider Technical Administrator                                                                                                      |
| Configuration_Wizard       | Cloud Provider Technical Administrator                                                                                                      |
| OrderPage_KnowledgeCenter  | Cloud Provider Technical Administrator<br>Organization Technical Administrator<br>Virtual and Physical Server Owner<br>Virtual Server Owner |
| OrderPage_OrderResource    | Cloud Provider Technical Administrator<br>Organization Technical Administrator<br>Virtual and Physical Server Owner<br>Virtual Server Owner |
| OrgAdmin_UserManagement    | Cloud Provider Technical Administrator<br>Organization Technical Administrator                                                              |
| Upgrade_Wizard             | Cloud Provider Technical Administrator                                                                                                      |
| VDC_Calculator             | Cloud Provider Technical Administrator                                                                                                      |
| <b>JavaScript folder:</b>  |                                                                                                                                             |
| Infrastructure_Discovery   | Cloud Provider Technical Administrator                                                                                                      |
| IPAMGroupFilterGrid        | Cloud Provider Technical Administrator                                                                                                      |
| IPAMNetworkCapacity        | Cloud Provider Technical Administrator                                                                                                      |
| Manage_MyErrorRemediations | Cloud Provider Technical Administrator<br>Organization Technical Administrator                                                              |
| Manage_MyServers           | Cloud Provider Technical Administrator<br>Organization Technical Administrator<br>Virtual and Physical Server Owner<br>Virtual Server Owner |

Table 4-1 Portlet Permissions (continued)

| Portlet                          | User Role (Read Only)                                                                                                                       |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Manage_MyVDCs                    | Cloud Provider Technical Administrator<br>Organization Technical Administrator                                                              |
| Report_SystemResourceCapacity    | Cloud Provider Technical Administrator                                                                                                      |
| Report_ViewCloudResourceUsage    | Cloud Provider Technical Administrator<br>Organization Technical Administrator<br>Virtual and Physical Server Owner<br>Virtual Server Owner |
| Report_ViewPodCapacity           | Cloud Provider Technical Administrator                                                                                                      |
| Connection_Status                | Cloud Provider Technical Administrator                                                                                                      |
| <b>Reserved Portlets folder:</b> |                                                                                                                                             |
| Approvals                        | Cloud Provider Technical Administrator<br>Organization Technical Administrator                                                              |
| OrderStatus                      | Cloud Provider Technical Administrator<br>Organization Technical Administrator<br>Virtual and Physical Server Owner<br>Virtual Server Owner |

Step 4 Proceed to [Adding the Approvals Portlet to the My Approvals Portal Page](#).

## Adding the Approvals Portlet to the My Approvals Portal Page

- Step 1 In **Portal Designer**, click the **Portal Pages** tab.
- Step 2 In the left navigation pane, in the Cisco IAC 3.1 folder, select the **My Approvals** portal page.
- Step 3 Select the **Portlets** tab.
- Step 4 Click **Add Portlets to Page**.
- Step 5 In the left navigation pane, expand the **Content Portlets** folder, then the **Reserved Portlets** subfolder.
- Step 6 Select the **Approvals** portlet and click **Add**.
- Step 7 Proceed to [Adding the OrderStatus Portlet to the My Orders Portal Page](#).

## Adding the OrderStatus Portlet to the My Orders Portal Page

- Step 1 In **Portal Designer**, click the **Portal Pages** tab.
- Step 2 In the left navigation pane, in the Cisco IAC 3.1 folder, select the **My Orders** portal page.
- Step 3 Select the **Portlets** tab.

- Step 4 Click **Add Portlets to Page**.
- Step 5 In the left navigation pane, expand the **Content Portlets** folder, then the **Reserved Portlets** subfolder.
- Step 6 Select the **OrderStatus** portlet and click **Add**.
- Step 7 Proceed to [Adding Portal Pages to My Workspace](#).

## Adding Portal Pages to My Workspace

Cloud Portal ships with reserved portlets for searching, orders, and approvals. Up to 10 tabs can be added to individual portals in My Workspace.



### Note

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 about hiding the buttons, see [Inactivate Reserved Portlet Buttons from the My Workspace Toolbar, page 8-23](#).

- Step 1 Open Cloud Portal and log in to the application as a Cloud Provider Technical Administrator.
- Step 2 Choose the **My Workspace** from the module drop-down list.

*Figure 4-12 My Workspace—Open Page*



- Step 3 Click + to display the Open Page dialog box.
- Step 4 Expand the **Cisco IAC**, **My Workspace**, or **System** folder.
- Step 5 Select a portal page and click **Open** to add a tab for that page. You can add up to 10 tabs.
- Step 6 Proceed to [Assign Additional Permissions for the Cloud Provider Technical Administrator Role](#).

## Assign Additional Permissions for the Cloud Provider Technical Administrator Role

Cisco IAC ships with permissions assigned to certain roles. However, you must manually assign additional permissions to the Cloud Provider Technical Administrator role.

## Set Read/Write Permissions for Organization Unit, Person, and Queue

- Step 1 Choose **Organization Designer** from the module drop-down list, then click the **Roles** tab.
- Step 2 Expand **Cisco Intelligent Automation for Cloud Roles** in the Role Hierarchy pane, and select **Cloud Provider Technical Administrator**.
- Step 3 From the right menu, select **Permissions** to open the Permissions Assigned to This Role pane.
- Step 4 Click **Add Permission**.
- Step 5 On the Add [Additional] Permissions pane, select the following filters, then click **Add**:

| Field                     | Action                                                  |
|---------------------------|---------------------------------------------------------|
| Object Type               | Choose Organizational Unit from the drop-down list.     |
| Permissions for this type | Choose Read/Write from the drop-down list.              |
| Assign permission to      | Click the <b>All objects of this type</b> radio button. |

**Figure 4-13** Organization Designer—Add [Additional] Permission

- Step 6 Repeat [Step 1](#) through [Step 5](#) for the Person and Queue object types.
- Step 7 Proceed to [Set Read Permissions for Managing Other Roles](#).

## Set Read Permissions for Managing Other Roles

- Step 1 Choose **Organization Designer** from the module drop-down list, then click the **Roles** tab.
- Step 2 Expand **Cisco Intelligent Automation for Cloud Roles** in the Role Hierarchy pane, and select **Cloud Provider Technical Administrator**.
- Step 3 From the right menu, select **Permissions** to open the Permissions Assigned to This Role pane.
- Step 4 Click **Add Permission**.

**Step 5** On the Add [Additional] Permission pane (Figure 4-13 on page 4-18), select the following filters:

| Field                     | Action                                          |
|---------------------------|-------------------------------------------------|
| Object Type               | Choose <b>Role</b> from the drop-down list.     |
| Permissions for this type | Choose <b>Read</b> from the drop-down list.     |
| Assign permission to      | Click the <b>Selected Objects</b> radio button. |

**Step 6** In the Roles pane, check the check boxes for the following objects *only*:

- Cloud Provider Technical Administrator
- Organization Technical Administrator
- Virtual and Physical Server Owner
- Virtual Server Owner
- Solutions Team
- Form Extender

**Figure 4-14** Organization Designer—Add Read Permission

The screenshot shows the 'Add [Additional] Permission' pane with the following configuration:

- Object Type:** Role
- Permissions for this type:** Read / Write
- Assign permission to:** Selected Objects (radio button selected)
- Search:** [Empty text box] Search

The 'Roles' pane displays a list of roles with checkboxes:

- Cisco Intelligent Automation for Cloud Roles
- Cloud Provider Technical Administrator
- Form Extender
- Organization Technical Administrator
- Searchability Role
- Solutions Team
- Virtual and Physical Server Owner
- Virtual Server Owner

At the bottom of the Roles pane, there are 'Add' and 'Cancel' buttons, a pagination control showing '1 - 8 of 8' items, and a 'Go' button.

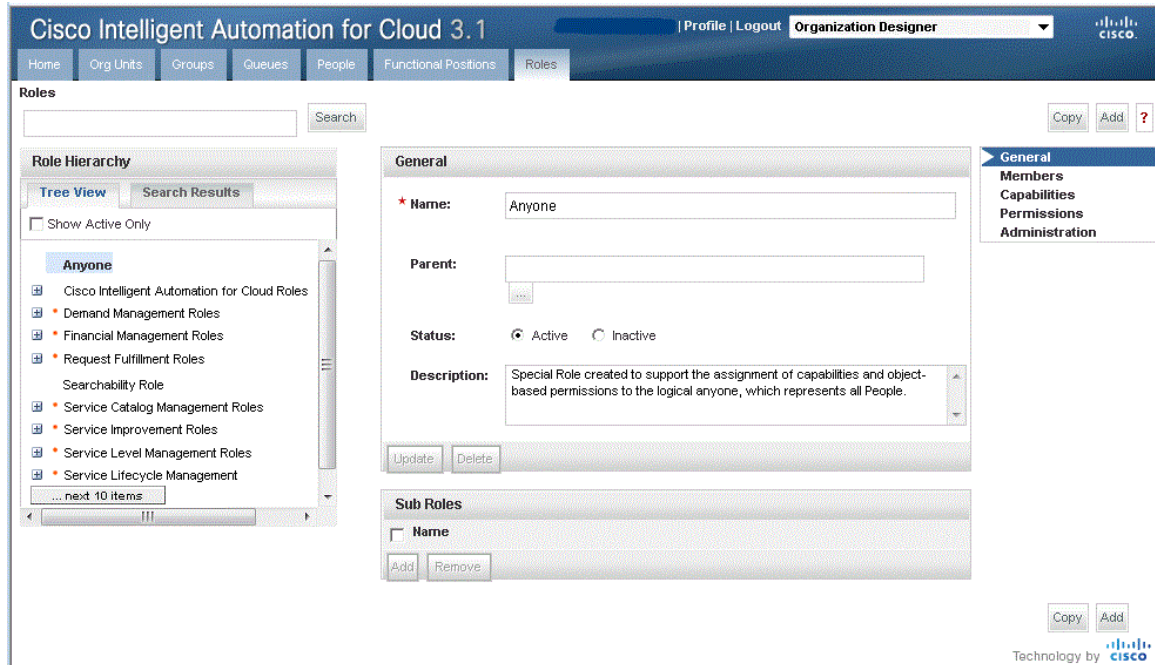
**Step 7** Click **Add**, then proceed to [Set Permissions for Service Queue Management](#).

## Set Permissions for Service Queue Management

These settings allow the Cloud Provider Technical Administrator role and the Organization Technical Administrator role permission to manage the roles delivered and used in the solution.

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

**Figure 4-15** Organization Designer—Roles



- Step 2** Expand **Cisco Intelligent Automation for Cloud Roles** in the Role Hierarchy pane, and select **Cloud Provider Technical Administrator**.
- Step 3** From the right menu, select **Permissions** to open the Permissions Assigned to This Role pane.
- Step 4** Click **Add Permission**.
- Step 5** On the Add [Additional] Permission pane (Figure 4-16 on page 4-21), select the following filters:

| Field                     | Action                                              |
|---------------------------|-----------------------------------------------------|
| Object Type               | Choose <b>Queue</b> from the drop-down list.        |
| Permissions for this type | Choose <b>Access Queue</b> from the drop-down list. |
| Assign permission to      | Click the <b>Selected Objects</b> radio button.     |

Figure 4-16 Organization Designer—Add Permission

The screenshot shows the Cisco Organization Designer interface. The main content area is titled 'Roles > Cloud Provider Technical Administrator'. On the left, there is a 'Role Hierarchy' pane with a tree view showing the role 'Cloud Provider Technical Administ' selected. Below it is a search bar and a 'Show Active Only' checkbox. The main area displays a table of 'Permissions Assigned to this Role' with columns for 'Name' and 'Type'. The table lists various permissions, all with a 'Read' type. At the bottom of the table, there is an 'Add Permission' button highlighted with a red box and a 'Remove' button. Below the table is a pagination control showing '1 - 20 of 105' items. On the right side, there is a sidebar with tabs for 'General', 'Members', 'Capabilities', 'Permissions', and 'Administration', with 'Permissions' currently selected. At the top right, there are 'Copy' and 'Add' buttons. At the bottom right, there are 'Copy' and 'Add' buttons.

**Step 6** In the Queues pane, check the check boxes for the following objects:

- Cloud Service Cancellation
- Cloud Service Delivery Management
- Cloud Service Lease Administration
- Cloud Service Remediation
- Default Service Delivery
- Cloud Service Approval Administration

**Step 7** Click **Add**.

**Step 8** Proceed to [Assign Additional Permissions for the Organization Technical Administrator Role](#).

# Assign Additional Permissions for the Organization Technical Administrator Role

Cisco IAC ships with permissions assigned to certain roles. However, you must manually assign additional permissions to the Organization Technical Administrator role.

## Assign Read Permissions for Role

The setting allows an Organization Technical Administrator to add other Organization Technical Administrators.

- 
- Step 1 Choose **Organization Designer** from the module drop-down list, then click the **Roles** tab.
  - Step 2 Expand **Cisco Intelligent Automation for Cloud Roles** in the Role Hierarchy pane, and click **Organization Technical Administrator**.
  - Step 3 In the right menu, select **Permissions** to open the Permissions Assigned to This Role pane.
  - Step 4 Click **Add Permission**.
  - Step 5 Add [Additional] Permission form, choose the following filters from the drop-down lists:
    - Object Type—**Role**
    - Permissions for this type—**Read**
    - Assign permission to—**Selected Objects**
  - Step 6 In the Roles pane, check the check box beside Organization Technical Administrator.
  - Step 7 Click **Add**, then proceed to [Assign Read Permissions for Person](#).
- 

## Assign Read Permissions for Person

The setting allows an Organization Technical Administrator to assign other Organization Technical Administrators and to manage people within the organization.

- 
- Step 1 Choose **Organization Designer** from the module drop-down list, then click the **Roles** tab.
  - Step 2 Expand **Cisco Intelligent Automation for Cloud Roles** in the Role Hierarchy pane, and select **Organization Technical Administrator**.
  - Step 3 From the right menu, select **Permissions** to open the Permissions Assigned to This Role pane.
  - Step 4 Click **Add Permission** to open the Add [Additional] Permission form.
  - Step 5 Select the following filters:
    - Object Type—**Person**
    - Permissions for this type—**Read**
    - Assign permission to—**All objects of this type**



**Step 6** Click **Add**, then proceed to [Assign Additional Permissions for the Server Owner Roles](#).

---

## Assign Additional Permissions for the Server Owner Roles

Cisco IAC ships with permissions assigned to certain roles. However, you must manually assign additional permissions to the following roles:

- Virtual Server Owner
  - Virtual and Physical Server Owner
- 

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

**Step 2** Expand **Cisco Intelligent Automation for Cloud Roles** in the Role Hierarchy pane.

**Step 3** For the Virtual and Physical Server Owner:

- In the right menu, select **Permissions** to open the Permissions Assigned to This Role pane.
- Click **Add Permission**.
- Select the following filters:
  - Object Type—**Person**
  - Permissions for this type—**Read**
  - Assign permission to—**All objects of this type**
- Click **Add**.

**Step 4** Repeat Step 3 for the Virtual Server Owner.

**Step 5** Click **Add**.

---





# CHAPTER 5

## Running the Configuration Wizard

---

The Cisco Intelligent Automation for Cloud Configuration Wizard is a portal that guides you through the critical steps for setting up and configuring the cloud administration and infrastructure. It reduces configuration time by providing access to the various forms and services from one location.



**Note**

The Configuration Wizard is optional. By using the Configuration Wizard, you can bypass the following two chapters for setting up cloud administration and infrastructure, with the following exceptions:

- Assign email addresses for queues (see [page 6-10](#))
  - Configure default email notification templates (see [page 6-12](#))
  - Configure and enable approvals (see [page 6-18](#))
- 



**Note**

If you prefer to complete the tasks individually instead of using the Configuration Wizard, skip to [Chapter 6, “Creating Cloud Administration Organization and Administrative Accounts.”](#)

---

This chapter provides instructions for using the Configuration Wizard and completing the forms. It contains the following sections:

- [Prerequisites](#)
- [Overview](#)
- [Getting Started](#)
- [Step 1: Agent Properties Configuration](#)
- [Step 2: Cloud Administration](#)
- [Step 3: Connect Cloud Infrastructure](#)
- [Step 4: POD Management](#)
- [Step 5: Set System-Wide Services and Provisioning Settings](#)
- [Step 6: Add Networks \(Optional\)](#)
- [Step 7: Create Shared Zone \(Optional\)](#)
- [Setup Complete](#)

# Prerequisites

Before you begin using the Configuration Wizard, you must have installed:

- Cisco Cloud Portal
- Cloud Portal Patch
- REX adapter

Additionally, the following tasks must be completed:

- Enable Web services (see [page 4-2](#)).
- Configure custom stylesheets (see [page 4-6](#)).
- Set permissions for portal pages and portlets ([page 4-12](#)).
- Configure and enable approvals ([page 4-23](#)).

If you have followed the sequence of steps presented in this guide, you should already have these requirements in place.

# Overview

The Configuration Wizard is a portal in My Workspace that walks you through a sequence of critical steps to set up and configure Cisco IAC.

The Configuration Wizard contains seven steps that provide access to forms for configuring requirements.

1. Agent Properties Configuration
2. Cloud Administration
3. Connect Cloud Infrastructure
4. POD Management
5. Set System-Wide Services and Provisioning Settings
6. Add Networks (optional)
7. Create Shared Zone (optional)

# Getting Started

To open the Configuration Wizard:

- 
- Step 1 Open Cloud Portal and log in as **Site Administrator**.
- Step 2 Choose **My Workspace** from the module drop-down list, then click the **Configuration Wizard** tab.

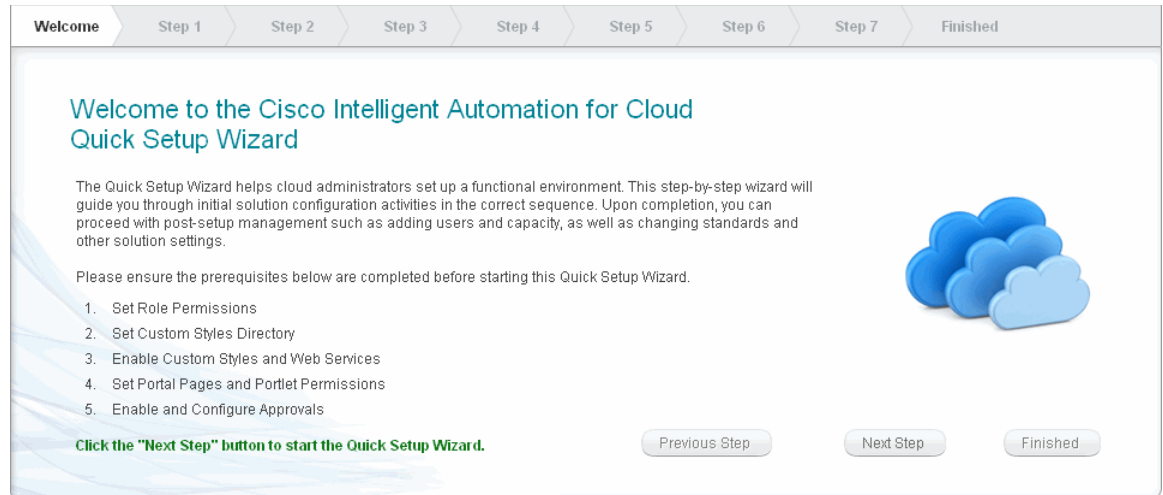


---

**Note** If you have not yet added portal access to My Workspace, see [Adding Portal Pages to My Workspace, page 4-17](#).

---

**Figure 5-1 Cisco IAC Configuration Wizard—Welcome and General Information**



- Step 3** Click on each of the links in steps 1-5 to ensure all the prerequisites have been met. Refer to the following sections for each step:
- a. Set Role Permissions (see [Add a Server Owner](#), page 9-4).
  - b. Set Custom Styles Directory (see [Configure Cloud Portal Stylesheets](#), page 4-6).
  - c. Enable Custom Styles and Web Services (see [Enable Web Services](#), page 4-2 and [Configure Cloud Portal Stylesheets](#), page 4-6).
  - d. Set Portal Pages and Portlet Permissions (see [Set Permissions for Portals and Portlets](#), page 4-12).
  - e. Enable and Configure Approvals (see [page 4-23](#)).
- Step 4** Click **Next Step**.

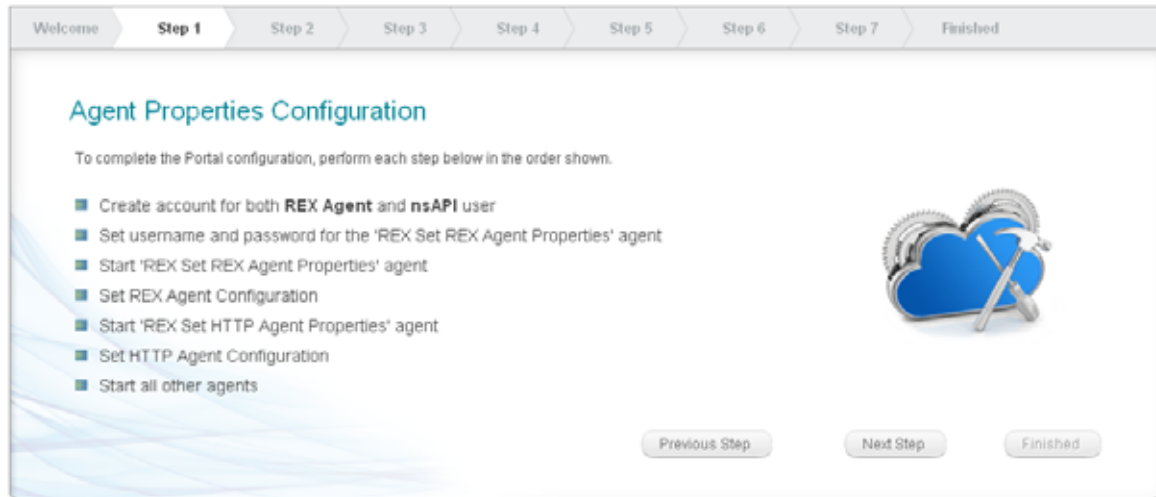
# Step 1: Agent Properties Configuration


**Note**

For Step 1, you must be logged in as the **Site Administrator**.

Configure agent properties for all REX agents, the CIM File agent, and HTTP agents.

**Figure 5-2** Configuration Wizard—Step 1: Agent Properties Configuration



For Step 1: Agent Properties Configuration, perform the following tasks:

- 
- Step 1 Create user accounts for both REX Agent and nsAPI users ([page 6-2](#)).
  - Step 2 Set the username and password for “REX Set REX Agent Properties” ([page 6-6](#)).
  - Step 3 Start the “REX Set REX Agent Properties” agent ([page 6-7](#)).
  - Step 4 Set the REX Agent Configuration properties ([page 6-7](#)).
  - Step 5 Start the “REX Set HTTP Agent Properties” agent ([page 6-8](#)).
  - Step 6 Start all other agents ([page 6-10](#)).
  - Step 7 When you have completed all of the tasks in Step 1, click **Next Step**.
-

## Step 2: Cloud Administration

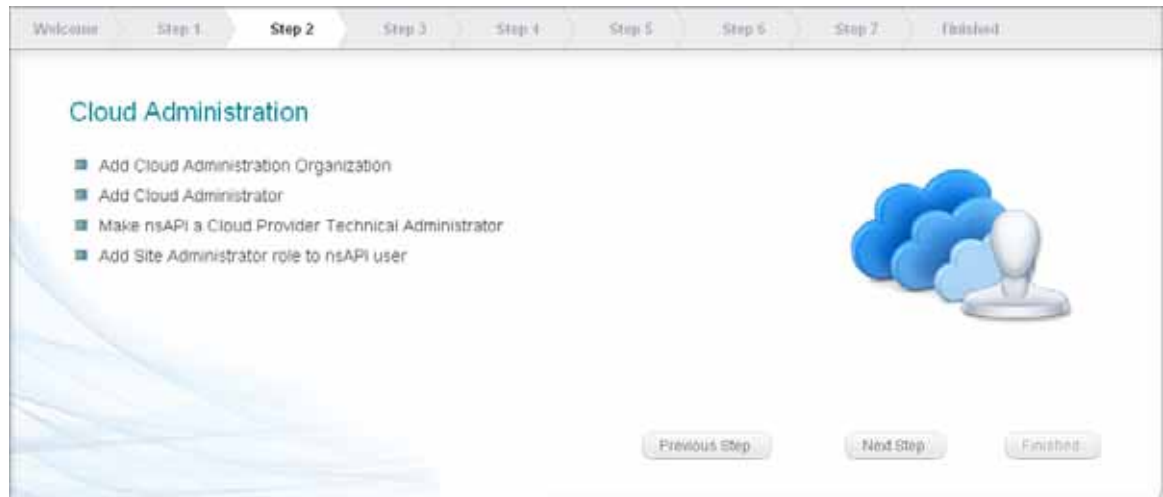


Note

For Step 2, you must be logged in as the **Site Administrator**.

Create the home organization for Cloud Provider Technical Administrators.

**Figure 5-3** Configuration Wizard—Step 2: Cloud Administration



For Step 2: Cloud Administration, perform the following tasks:

- 
- Step 1** Create the Cloud Provider Technical Administrator home organization unit ([page 6-15](#)).
  - Step 2** Create a Cloud Administrator ([page 6-15](#)).
  - Step 3** Make nsAPI a Cloud Provider Technical Administrator ([page 6-17](#)).
  - Step 4** Add Site Administrator role to nsAPI user ([page 6-18](#)).
  - Step 5** When you have completed all of the tasks in Step 2, click **Next Step**.
-

## Step 3: Connect Cloud Infrastructure

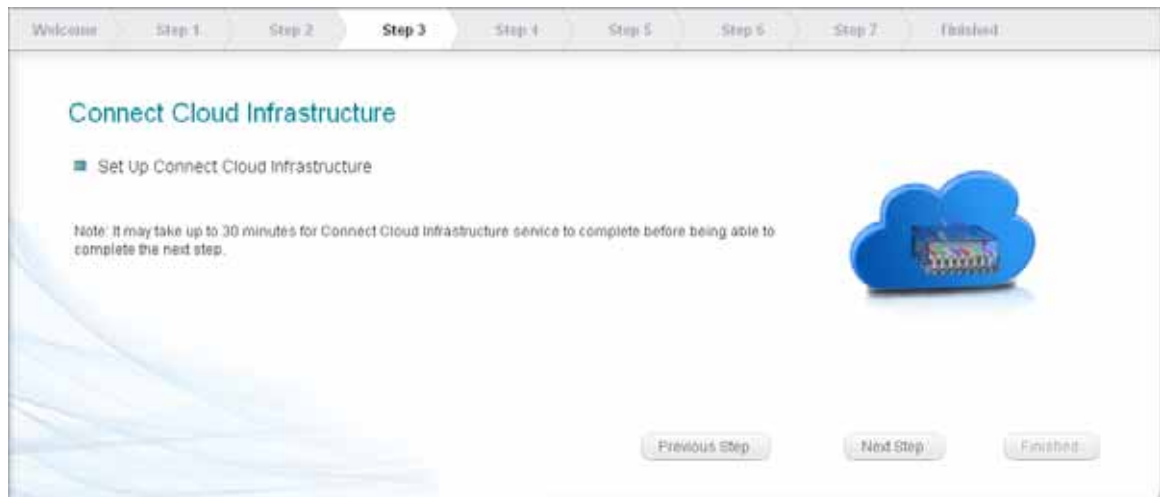


### Note

Before beginning Step 3, you must log out, close your browser, then log back in as a **Cloud Provider Technical Administrator**.

This step defines the connection information for the platform elements that will be used in Cisco IAC. This information will be used by Tidal Enterprise Orchestrator (TEO) to integrate with the various components involved in the cloud provisioning processes.

**Figure 5-4** Configuration Wizard—Step 3: Connect Cloud Infrastructure



For Step 3: Connect Cloud Infrastructure, perform the following tasks:

- 
- Step 1** Click **Next Step** to start the discovery process that sets up the cloud infrastructure. The process can take from 30 to 45 minutes to complete.
  - Step 2** When the discovery process is complete, click **Next Step**.
-



## Step 4: POD Management



Note

For Step 4, you must remain logged in as a **Cloud Provider Technical Administrator**.

Create the Point-of-Delivery (POD) and select the instances that manage its resources.

*Figure 5-5 Configuration Wizard—Step 4: POD Management*



For Step 4: POD Management, perform the following tasks:

- Step 1** Create the POD and select the resources that manage its resources ([page 7-11](#)).
- Step 2** When you have completed Step 4, click **Next Step**.

## Step 5: Set System-Wide Services and Provisioning Settings

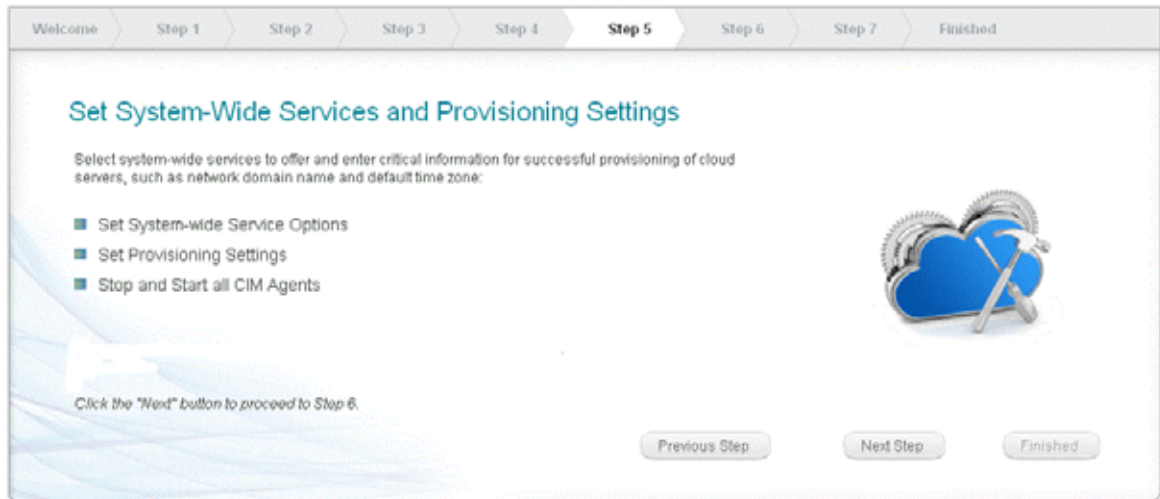


### Note

For Step 5, you must remain logged in as a **Cloud Provider Technical Administrator**.

Select the system-wide services to offer and enter critical information for provisioning the cloud servers, such as network domain name and default time zone.

**Figure 5-6** Configuration Wizard—Step 5: Set Provisioning Settings



For Step 5: Set System-Wide Services and Provisioning Settings, perform the following tasks:

- 
- Step 1** Set the system-wide service options ([page 7-7](#)).
  - Step 2** Stop and start and stop all CIM agents ([page 7-10](#)).
  - Step 3** When you have completed Step 5, click **Next Step**.
-

## Step 6: Add Networks (Optional)

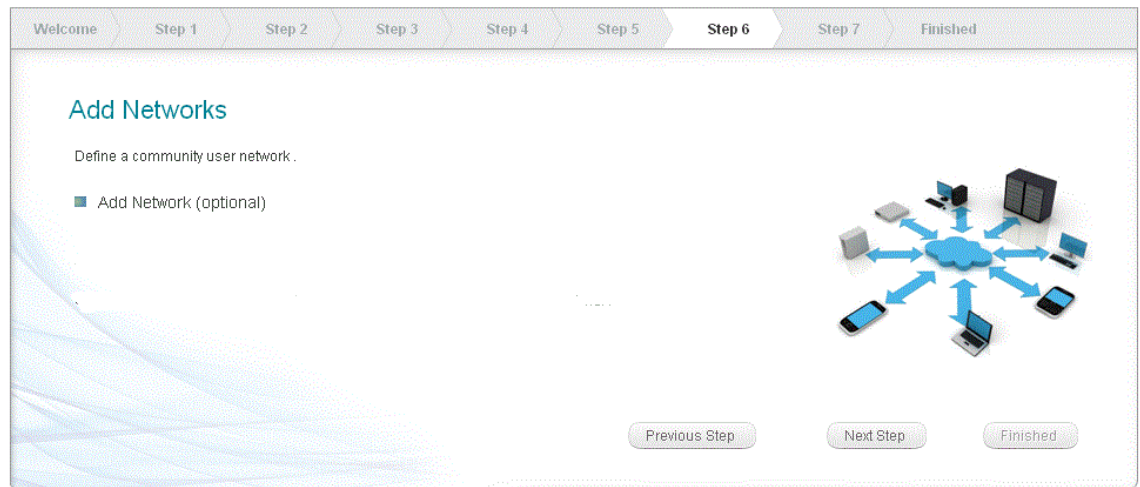


Note

For Step 6, you must remain logged in as a **Cloud Provider Technical Administrator**.

Optionally, add community and user networks to which users can deploy servers, management networks, and infrastructure networks to be used for bare metal provisioning.

**Figure 5-7** Configuration Wizard—Step 6: Add Network



For Step 6: Add Networks, perform the following tasks:

- 
- Step 1** Add a community or user network ([page 8-21](#)).
  - Step 2** Add an infrastructure network ([page 8-21](#)).
  - Step 3** Add a management network ([page 8-21](#)).
  - Step 4** When you have completed all of the tasks in Step 6, click **Next Step**.
-

## Step 7: Create Shared Zone (Optional)

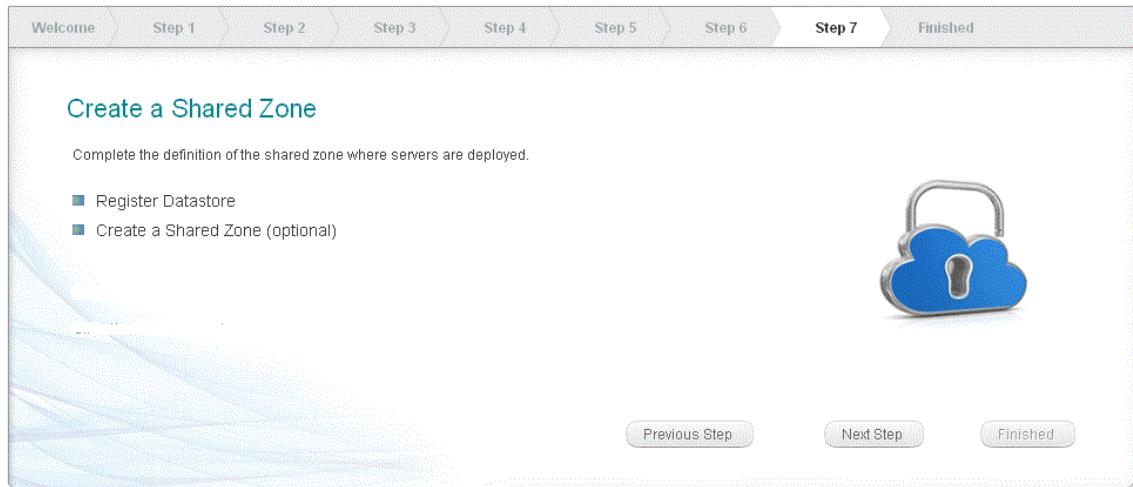

**Note**

For Step 7, you must remain logged in as a **Cloud Provider Technical Administrator**.

Complete the definition of the shared zone where servers are deployed. This includes:

- Registering this datastore to be available for virtual data centers.
- Creating a shared deployment environment in which all users can deploy servers.

**Figure 5-8** Configuration Wizard—Step 7: Set Up Shared Zone



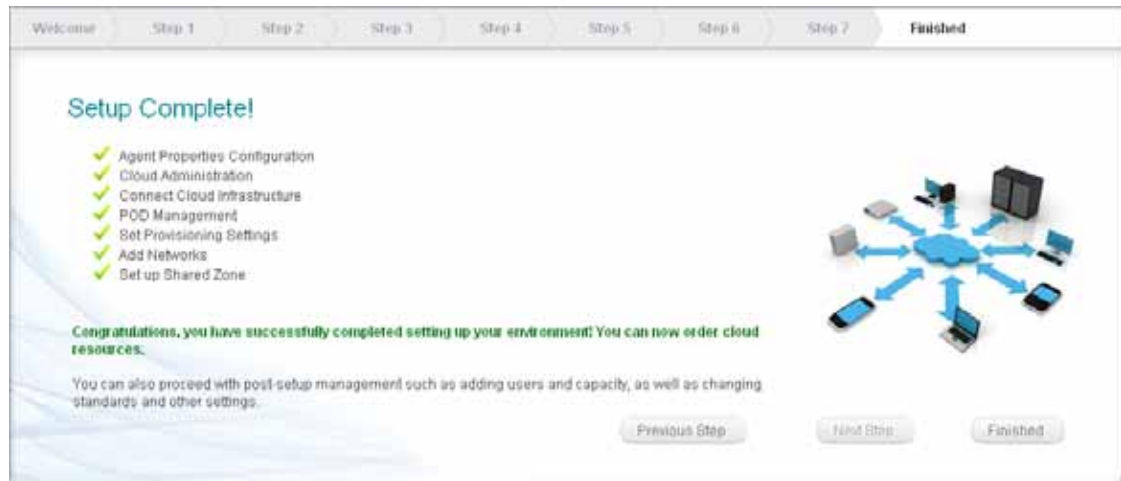
For Step 7: Set Up Shared Zone, perform the following tasks:

- 
- Step 1** Register the datastore ([page 7-12](#)).
- Step 2** Complete the definition of the shared zone where servers are deployed ([page 7-13](#)).
- Step 3** When you have completed all of the tasks in Step 7, click **Next Step**.
-

# Setup Complete

You have completed the Configuration Wizard, and your cloud environment is now set up for ordering.

**Figure 5-9** Configuration Wizard—Setup Complete



You can now skip to one of the following chapters:

- [Chapter 8, “Post-Configuration Options”](#)—*Optional*. Configure additional networks, UCS blades, and templates, and modify ordering standards (for example, available server sizes) to present to users as options. If you choose not to configure these items now, you or any administrator can set up any of these services at any time after the cloud system is in use by users. After you are finished, proceed to [Chapter 9, “Setting Up an Organization and Adding Users.”](#)
- [Chapter 9, “Setting Up an Organization and Adding Users”](#)—*Required*. Create organizations, and add additional Cloud Administrators, Organization Technical Administrators, and Server Owners. These are the groups who will log in and use Cloud Portal.





# CHAPTER 6

## Creating Cloud Administration Organization and Administrative Accounts

---



Note

If you used the Cisco IAC Quick Setup Wizard, you have already completed the tasks in this chapter and in the following chapter. Skip to [Chapter 8, “Post-Configuration Options,”](#) for optional configurations, or to [Chapter 9, “Setting Up an Organization and Adding Users,”](#) to resume required configuration.

---



Note

Before you can perform the tasks in this chapter, you **MUST** complete **all** of the tasks, in sequence, that are presented in the previous chapters.

---

After performing the set up and deployment tasks covered in the previous chapters, you must now create a home organization for Cloud Administrators, then add a Cloud Administrator. This chapter guides you through those processes. It includes the following tasks:

- [Set Up REX and nsAPI User Accounts](#)
- [Configure Agent Properties](#)
- [Assign Mail Addresses for Queue Notifications](#)
- [Configure the Email Notification Templates](#)
- [Create the Cloud Provider Technical Administrator Organization](#)
- [Add Cloud Provider Technical Administrators](#)
- [Configure and Enable Approvals](#)



Note

Complete every task this chapter exactly as instructed and in the sequence that is presented. **Do not skip sections.**

---

## Set Up REX and nsAPI User Accounts

Create user accounts for REX adapter and nsAPI that will be used to connect Cloud Portal to the REX adapter and Tidal Enterprise Orchestrator, respectively.



### Note

You created the nsAPI username and password when you imported and configured the Intelligent Automation for Cloud Starter Automation Pack into CPO. (See [Import and Configure the Intelligent Automation for Cloud Starter Automation Pack, page 2-14](#)). You will now create the user account for nsAPI using those credentials.

**Step 1** Choose **Organization Designer** from the module drop-down list.

**Step 2** On the Organization Designer home page, click **Create Person** in the Common Tasks pane.

**Figure 6-1** Create Person Form

The screenshot shows the 'Create Person' form within the Organization Designer application. The form is titled 'Create Person' and has a 'Close' button in the top right corner. The form contains several input fields, each with a red asterisk indicating it is a required field. The fields are: First Name, Last Name, Email, Time Zone (a dropdown menu currently showing '(GMT-08:00) Pacific Time (US and Canada), Tijuana'), Language (a dropdown menu currently showing 'US English'), Home OU (with a search icon), Login, Password, and Confirm Password. There is also a 'Notes' field with a scroll bar. At the bottom of the form, there are 'Create' and 'Cancel' buttons.



### Note


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

**Step 3** **Set up the REX user account:**

On the Create Person form, provide the following information:

| Field      | Action                                                                                                                                               |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| First Name | Enter a first and last name for the REX user. It is recommended that you choose something that is easy to remember, for example, "rex user."         |
| Last Name  |                                                                                                                                                      |
| Email      | Enter a valid, actively monitored email address. This will be the address where notifications relating to the REX adapter user account will be sent. |



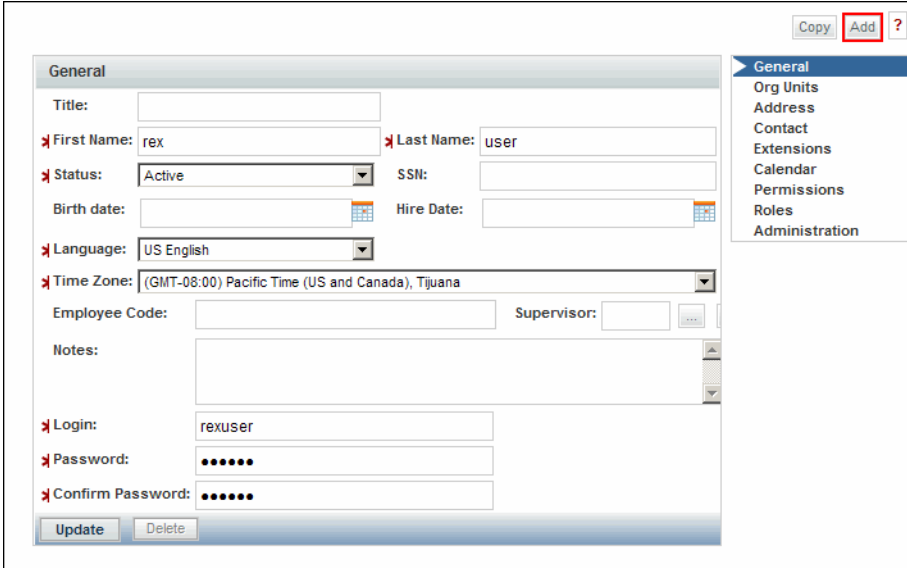
| Field                        | Action                                                                                                                                                                                                                                                                |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time Zone                    | Choose <b>(GMT) Greenwich Mean Time</b> from the drop-down list.<br><b>Note</b> This setting is mandatory.                                                                                                                                                            |
| Language                     | Leave as is. In the current release, only US English is supported; any language selection you make will be ignored.                                                                                                                                                   |
| Home OU                      | Click the <b>Browse</b>  tool to open the Select an Organizational Unit dialog box. Click <b>Search</b> , click the <b>Site Administration</b> radio button, then click <b>Add</b> . |
| Notes                        | <i>Optional.</i> Enter a description or any information pertinent to the REX user account.                                                                                                                                                                            |
| Login                        | Enter <b>rexuser</b> .                                                                                                                                                                                                                                                |
| Password<br>Confirm Password | Enter, then re-enter a password for the REX adapter user account.                                                                                                                                                                                                     |

**Step 4** Click **Create** to submit and close the form.

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

**Step 5** Click **Add** in the upper right corner to add the REX user account.

**Figure 6-2 Add Another Person**



The screenshot shows a web form for adding a new person. The form is titled "General" and has a sidebar on the right with a menu containing: General, Org Units, Address, Contact, Extensions, Calendar, Permissions, Roles, and Administration. The "Add" button in the top right corner is highlighted with a red box. The form fields are as follows:

- Title:
- First Name:  Last Name:
- Status:  SSN:
- Birth date:  Hire Date:
- Language:
- Time Zone:
- Employee Code:  Supervisor:
- Notes:
- Login:
- Password:
- Confirm Password:


At the bottom of the form are "Update" and "Delete" buttons.



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

**Step 6** Set up the nsAPI user account:

On the Create Person form (Figure 6-1 on page 6-2), provide the following information:

| Field                                 | Action                                                                                                                                                                                                                                                                |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| First Name<br>Last Name               | Enter a first and last name for the nsAPI user. You can specify a person's name or something that is easy to identify, for example, "nsapi user." It is recommended that you specify an easily identifiable name if the login will be used by multiple people.        |
| Email                                 | Enter a valid, actively monitored email address. This will be the address where notifications relating to the nsAPI user account will be sent.                                                                                                                        |
| Time Zone                             | Choose <b>(GMT) Greenwich Mean Time</b> from the drop-down list.<br><b>Note</b> This setting is mandatory.                                                                                                                                                            |
| Language                              | Leave as is. In the current release, only US English is supported; any language selection you make will be ignored.                                                                                                                                                   |
| Home OU                               | Click the <b>Browse</b>  tool to open the Select an Organizational Unit dialog box. Click <b>Search</b> , click the <b>Site Administration</b> radio button, then click <b>Add</b> . |
| Notes                                 | <i>Optional.</i> Enter a description or any information pertinent to the nsAPI user account.                                                                                                                                                                          |
| Login<br>Password<br>Confirm Password | Enter the username, and enter and confirm the password for the nsAPI user account that you created in <a href="#">Step 3 of Import and Configure the Intelligent Automation for Cloud Starter Automation Pack, page 2-14</a> .                                        |

**Step 7** Click **Create** to close the form and return to Organization Designer.



**Note** In the next steps, you will set the calendar for the nsAPI user.

**Step 8** In Organization Designer, click the **People** tab.

**Step 9** In the People pane on the left side of the window, locate and click the name of the nsAPI user.

**Step 10** From the menu on the left side of the page, choose **Calendar**.

**Step 11** In the Calendar pane, change all time values in the **To** column to **11:59 PM**.

Figure 6-3 Organization Designer—Calendar

| Day       | From     | To       |
|-----------|----------|----------|
| Sunday    | 12:00 AM | 11:59 PM |
| Monday    | 12:00 AM | 11:59 PM |
| Tuesday   | 12:00 AM | 11:59 PM |
| Wednesday | 12:00 AM | 11:59 PM |
| Thursday  | 12:00 AM | 11:59 PM |
| Friday    | 12:00 AM | 11:59 PM |
| Saturday  | 12:00 AM | 11:59 PM |

Step 12 Click **Update** to submit the form.

## Configure Agent Properties

Configure agent properties for all REX agents and HTTP agents in the following sections:

- Set username and password for REX Set REX agent properties
- Start REX Set REX Agent Properties and REX Set HTTP Agent Properties agents
- Set REX Agent Configuration
- Set HTTP Agent Configuration
- Start all other agents



### Note

The CIM File Agent will be automatically configured when you set provisioning settings later in the setup and configuration process.

## Set Username and Password for REX Set REX Agent Properties

- Step 1** Choose **Service Link** from the module drop-down list, then click the **Manage Integrations** tab.
- Step 2** In the Agents pane on the left, expand **REX Set REX Agent Properties** and click **Outbound Properties**.

**Figure 6-4** REX Set REX Agent Properties

| Name                                     | Value                                           |
|------------------------------------------|-------------------------------------------------|
| REXOutboundAdapter.RoutingURL            | http://localhost:8088/RequestCenter             |
| REXOutboundAdapter.Username              | .....                                           |
| REXOutboundAdapter.Password              | .....                                           |
| REXOutboundAdapter.TimeOut               | 180000                                          |
| REXOutboundAdapter.Operation             | ModifyAgentProperty                             |
| REXOutboundAdapter.IsProcessResponse     | true                                            |
| REXOutboundAdapter.RefFieldXPath         | /rex/Agents/Agent/Transaction/@actionResultCode |
| REXOutboundAdapter.RefFieldPattern       | 0                                               |
| REXOutboundAdapter.CancelIdentifierXPath | /message/task-canceled                          |

- Step 3** In the REXOutboundAdapter.Username field, enter the REX login name that you created in the Create Person form.
- Step 4** In the REXOutboundAdapter.Password field, enter the REX password in the Create Person form.
- Step 5** Click **Save**, then proceed to [Start the REX Set Agent Properties Agent](#).

## Start the REX Set Agent Properties Agent

**Step 1** Choose **Service Link** from the module drop-down list, then click the **Control Agents** tab to open the portal.

The Control Agents portal displays a list of all agents.

**Step 2** Click the red icons ● next to **REX Set REX Agent Properties**, then click **Start Selected**.



**Note** If you do not see REX Set REX Agent Properties in the list, scroll down, or sort by agent name by clicking the Name column heading.

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

**Step 3** Proceed to [Set REX Agent Configuration](#).

## Set REX Agent Configuration

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

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

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

**Step 3** On the Agent Properties Configuration portlet, click **Set REX Agent Configuration** to open the form.

*Figure 6-5 Set REX Agent Configuration Form*

**Set REX Agent Configuration**  
Configure agent properties for REX agents. This sets up the agent properties for all the IAC REX agents.

Submit Order Reset

**Set REX Agent Configuration**

\* REX User Name:  Enter the user name for the Cloud Portal REX user.

\* REX Password:  Enter the password for the Cloud Portal REX user.

\* Confirm REX Password:  Enter the password for the Cloud Portal REX user again for password confirmation.

Submit Order Reset

- Step 4** On the Set REX Agent Configuration form, enter the REX account login name, then enter and re-enter the REX account password.
- Step 5** Click **Submit Order** to submit the form and display the Order Confirmation page for the service that you ordered. **Do not close the order confirmation.**

**Figure 6-6 Set REX Agent Configuration—Order Confirmation**

Your order has been submitted successfully. Please use the requisition number to communicate with service personnel about this order.

| Requisition Details        |                    |                      |                    |
|----------------------------|--------------------|----------------------|--------------------|
| <b>Requisition Number:</b> | 10712              | <b>Initiator:</b>    | Sue Jarocki(Cisco) |
| <b>Customer:</b>           | Sue Jarocki(Cisco) | <b>Created Date:</b> | 10/27/2012         |
| <b>Bill To:</b>            | IAC Development    | <b>Submit Date:</b>  | 10/27/2012         |


| Services                                                                             |                           |                   |          |           |                         |
|--------------------------------------------------------------------------------------|---------------------------|-------------------|----------|-----------|-------------------------|
| Name                                                                                 | Service Level Description | Standard Duration | Quantity | Unit Cost | Subtotal                |
| Set REX Agent Configuration                                                          |                           | Not Defined       | 1        | 0.00      | 0.00                    |
| Set REX Agent Configuration Pre-servicing [included in Set REX Agent Configuration]  |                           | Not Defined       | 1        | 0.00      | 0.00                    |
| Set REX Agent Configuration Post-servicing [included in Set REX Agent Configuration] |                           | Not Defined       | 1        | 0.00      | 0.00                    |
|                                                                                      |                           |                   |          |           | <b>Total Cost: 0.00</b> |

\*Standard Duration applies to delivery after any required authorizations have been completed.

| Delivery Process                                                |                    |                    |             |
|-----------------------------------------------------------------|--------------------|--------------------|-------------|
| Process Milestone                                               | Due Date           | Completed On       | Status      |
| <input checked="" type="checkbox"/> Service Group Authorization | 10/27/2012 8:09 AM | 10/27/2012 8:09 AM | Completed   |
| Delivery project for Set REX Agent Configuration                | 10/29/2012 9:00 AM |                    | In Progress |

- Step 6** In the Requisition Details pane, click the requisition number to open the requisition summary page.
- Step 7** Click **Comments & History** in the menu on the right side of the window.
- Step 8** In the System History pane, look for errors.
- If the REX agents are configured correctly, you will see a message for each agent stating that it was updated successfully.
- Step 9** Close the Comments and History window, then proceed to [Start the REX Set HTTP Properties Agent](#).

## Start the REX Set HTTP Properties Agent

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



**Note** If you do not see REX Set HTTP Agent Properties in the list, scroll down, or sort by agent name by clicking the Name column heading.

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

Step 3 Proceed to [Set HTTP Agent Configuration](#).

## Set HTTP Agent Configuration

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

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

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

Step 3 On the System Settings portlet, click Set HTTP Agent Configuration to open the form.



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

Step 4 On the Set HTTP Agent Configuration, provide following information:

| Field                                                                  | Action                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process Orchestrator Hostname                                          | Enter the fully qualified hostname or IP address of the TEO server. For example, teo01.cisco.com or 192.168.100.101.                                                                                                                                                                                                                                                                                                   |
| Authentication Scheme                                                  | Choose the one of the following two HTTP authentication schemes from the drop-down list: <ul style="list-style-type: none"> <li>• <b>NTLM—Default.</b> Authentication protocol that is used on networks that include systems running the Windows operating system and on stand-alone systems</li> <li>• <b>Basic—Standard method</b> that provides a user name and password to the authentication mechanism</li> </ul> |
| Process Orchestrator Username                                          | Enter the Windows username that will be used to connect to the TEO server.                                                                                                                                                                                                                                                                                                                                             |
| Process Orchestrator Password<br>Confirm Process Orchestrator Password | Enter, then re-enter the password associated with the TEO username.                                                                                                                                                                                                                                                                                                                                                    |
| Process Orchestrator Domain                                            | Enter the Windows domain for the TEO user.                                                                                                                                                                                                                                                                                                                                                                             |
| Cloud Portal Hostname                                                  | Enter the fully qualified hostname or IP address of Cloud Portal. For example, cp01.cisco.com or 192.168.100.102.                                                                                                                                                                                                                                                                                                      |

Step 5 Click **Submit Order** to submit the form and display the Order Confirmation page for the service that you ordered. **Do not close the order confirmation.**


Step 6 In the Requisition Details pane on the Order Confirmation page, click the requisition number to open the requisition summary page.

Step 7 Click **Comments & History** in the menu on the right side of the window.

Step 8 In the System History pane on the Comments and History page, look for errors. If the HTTP agents are configured correctly, you will see a message that the agent was updated successfully.

Step 9 Close the Comments and History window, then proceed to [Start All Other Agents](#).


## Start All Other Agents

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



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

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

- Step 3** If there are additional agents in the list, use the scroll arrow  at the bottom of the list to display to them, then repeat [Step 2](#).
- Step 4** Proceed to [Assign Mail Addresses for Queue Notifications](#).

## Assign Mail Addresses for Queue Notifications

You must update the queue configuration settings with email addresses that will receive email notifications for changes in service queues.

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

Cisco IAC ships with the following preconfigured queues:

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

Cloud Provider Technical Administrators and Organization Technical Administrator monitor, assign, or address tasks added to the queues. Those users with access to the queues can perform the tasks added the queues. When a task is added to a queue or is assigned or reassigned to a user, the designated users receive email notifications.



**Note** For information about working with queues, see the [Cisco Intelligent Automation for Cloud 3.1 User Guide](#).

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





**Tip** Use mailing lists (aliases), not specific user email addresses.

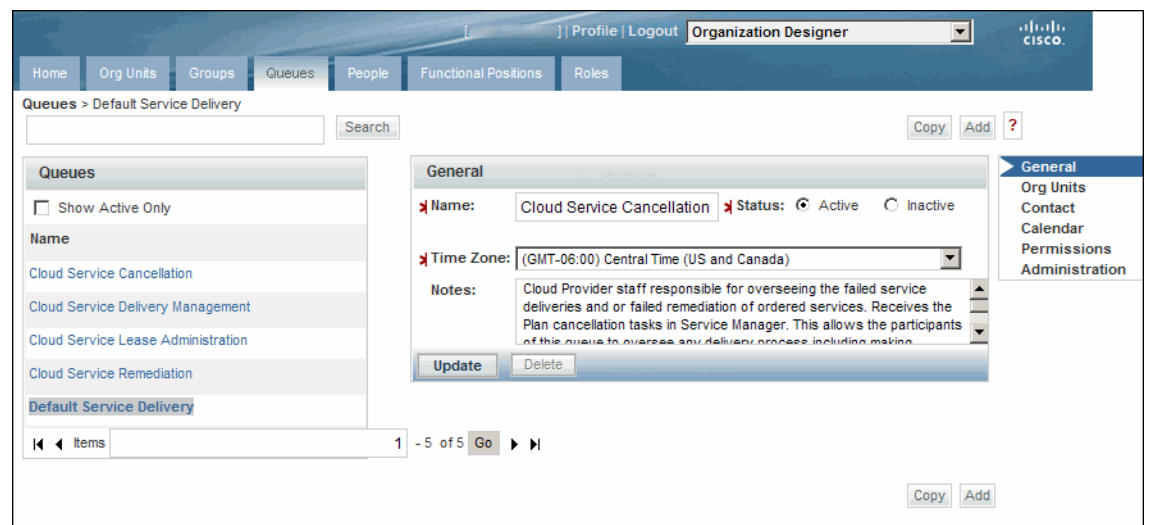


**Note** You must configure email addresses for each queue.

To specify email addresses to queues, complete the following steps.

- Step 1** Log in to Cloud Portal as an administrator.
- Step 2** Choose **Organization Designer** from the module drop-down list, then click the **Queues** tab.

**Figure 6-7** Organization Designer—Cloud Service Remediation Queue



- Step 3** In the Queues pane, click **Default Service Delivery**.
- Step 4** From the menu on the right side of the window, click **Contact** to display the Contact pane. Before configuration, the Contacts panel lists one test email address (typically, CloudServiceRemediation@domain.com).

Figure 6-8 Organization Designer—Cloud Service Remediation Queue Contact Information

The screenshot shows the 'Organization Designer' interface. The top navigation bar includes 'Home', 'Org Units', 'Groups', 'Queues', 'People', 'Functional Positions', and 'Roles'. The 'Queues' section is active, displaying a list of queues: 'Cloud Service Cancellation', 'Cloud Service Delivery Management', 'Cloud Service Lease Administration', 'Cloud Service Remediation', and 'Default Service Delivery'. The 'Default Service Delivery' queue is selected. A 'Contact' form is open, showing a table with columns 'Type' and 'Value'. The 'Email' type is selected, and the value is 'CloudServiceRemediation@domain.com'. There are 'Update', 'Add New', and 'Delete' buttons. A sidebar on the right shows a menu with 'General', 'Org Units', 'Contact', 'Calendar', 'Permissions', and 'Administration'. The 'Contact' option is selected. At the bottom, there are 'Copy' and 'Add' buttons.

- Step 5 Click in the Value field and edit the email address.
- Step 6 Click **Update**.
- Step 7 Repeat [Step 1](#) through [Step 6](#) to add additional email addresses to the queue.
- Step 8 Repeat [Step 3](#) through [Step 6](#) for the remaining queues.
- Step 9 Proceed to [Configure the Email Notification Templates](#).

## Configure the Email Notification Templates

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.

Before users can start ordering cloud services, you **must** configure the email notification templates with the relevant sender and recipient addresses.

To modify the default email notification templates, complete 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, click the **System Settings** tab.
- Step 3 On the System Settings portlet, click **Modify Email Templates** to open the form ([Figure 6-9 on page 6-13](#)).
- Step 4 On the Request Center tab in the Email Templates panel, update the following templates (the others are programmed using a service):
  - Ad-Hoc Task Started
  - Default Late Activity
  - My Services Departmental Reviews
  - My Services Financial and Departmental Authorizations

- My Services Service Group Authorizations
- My Services Service Group Reviews
- Process Escalation
- Service Link Error on External Task

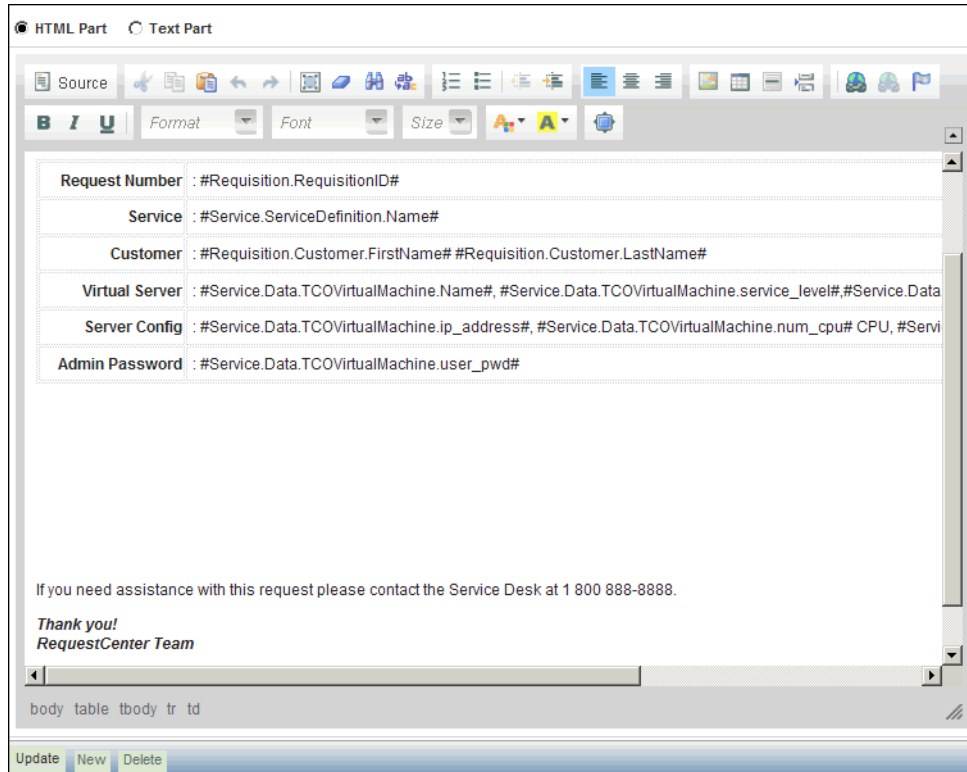
**Step 5** In the General pane, modify any or all of the following attributes:

| 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.<br><br><b>Note</b> You can use namespace variables in this field. For information on using namespaces, see the <i>Cisco Service Portal 9.1 Namespace Users Guide</i> . |
| Language | Leave as is. In the current release, only US English is supported; any language selection you make will be ignored.                                                                                                                                                                            |
| Type     | Click the <b>Request Center</b> radio button.                                                                                                                                                                                                                                                  |

**Figure 6-9** Email Templates Form

- Step 6** For the editing window, click one of the following radio buttons to choose an editor.
- **HTML Part** (shown in [Figure 6-9 on page 6-13](#))
  - **Text Part** (shown in [Figure 6-10 on page 6-14](#))
- Step 7** In the editing panel, modify the default content and add optional content as needed.

**Figure 6-10** 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.
- Step 10** Proceed to [Create the Cloud Provider Technical Administrator Organization](#).

# Create the Cloud Provider Technical Administrator Organization

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

**Step 2** On the System Setup portal, click the **Administrators** tab.

The Cloud Administrators portlet displays by default.

**Step 3** On the Administrators portlet, click **Modify Cloud Administration Organization** to open the form.



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



**Caution** For Cisco IAC, vCenter object names cannot contain forward slashes. If any of your vCenter object names contains forward slashes, please rename the files before you specify a vCenter path. For more information, please see the [VMware Software Preparation, page 1-9](#).

**Step 4** On the Add Cloud Administration Organization form, enter the following information:

| Field                         | Action                                                    |
|-------------------------------|-----------------------------------------------------------|
| Cloud Admin Organization Name | Enter <b>Cloud Provider Technical Administrator</b> .     |
| Organization Description      | <i>Optional.</i> Enter a description of the organization. |

**Step 5** Click **Submit Order**.

**Step 6** Proceed to [Add Cloud Provider Technical Administrators](#).

## Add Cloud Provider Technical Administrators

- [Add Cloud Administrators in the Directory Service \(If Applicable\)](#)—Refer to this section for information on how Cloud Administrators are imported and granted authorization during directory integration.
- [Manually Add Cloud Administrators \(Without Directory Service\)](#)—Follow this procedure if you are *not* using a directory service.
- [Manually Make nsAPI a Cloud Administrator \(Without Directory Service\)](#)—Follow this procedure to make the nsAPI user a Cloud Administrator.
- [Manually Add Site Administrator Role to nsAPI user \(Without Directory Service\)](#)—Follow this procedure to add the Site Administrator role to the nsAPI user.

## Add Cloud Administrators in the Directory Service (If Applicable)



Note

This section applies only if you are using a directory service to import user and organization data.



Note

Before you proceed, directory integration must be set up. For instructions on setting up directory integration, see [Appendix A “Setting Up Directory Integration.”](#)

After you set up directory integration, users are automatically imported when they log in, and their Cloud Portal roles are automatically assigned based on the user groups to which they were added in the directory. User roles are assigned when you define group role-mappings during directory integration setup (as shown in [Add the nsAPI User to the Cloud Administration Group, page A-9](#) in [Appendix A, “Setting Up Directory Integration”](#)).

You assign the Cloud Administrator role to a user from the directory, rather than from Cloud Portal, by adding the user to the Cloud Administrator user group in the directory.

Skip to [Chapter 7, “Setting Up the Cloud Infrastructure.”](#)

## Manually Add Cloud Administrators (Without Directory Service)



Note

If you are using a directory service to import the Cloud Administrator, see the information in the following section, [Add Cloud Administrators in the Directory Service \(If Applicable\), page 6-16](#).

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

**Figure 6-11** Add Cloud Administrator Form



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

**Step 3** On the Add Cloud Administrator form, choose **Create New User** from the Action drop-down list to display the fields for creating a new user as a Cloud Administrator.

**Step 4** Provide the following information:

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

**Step 5** Make nsAPI a Cloud Provider Technical Administrator ([page 6-17](#)).

**Step 6** Add Site Administrator role to nsAPI user ([page 6-18](#)).

**Step 7** Click **Submit Order**.

**Step 8** To create additional Cloud Administrators, repeat [Step 3](#) through [Step 7](#).

## Manually Make nsAPI a Cloud Administrator (Without Directory Service)



**Note** If you are using a directory service to import the Cloud Administrator, see the information in the following section, [Add Cloud Administrators in the Directory Service \(If Applicable\)](#), [page 6-16](#).

**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.

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

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

**Step 4** Select the nsAPI user.

**Step 5** Click **Submit Order**.

## Manually Add Site Administrator Role to nsAPI user (Without Directory Service)



### Note

If you are using a directory service, see the information in the following section, [Add Cloud Administrators in the Directory Service \(If Applicable\)](#), page 6-16.

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

## Configure and Enable Approvals

Authorizations are any approvals required in conjunction with completing fulfillment of a service request. Authorizations give the approver the opportunity to determine if the person requesting the service is eligible to receive it. If an authorization is rejected, the requisition will be canceled and the service will not be delivered.

A requisition that needs authorization will be placed in a queue specifically created for approvals. A queue for approvals is created whenever a new organization is created. Both the Organization Technical Administrator and the Cloud Provider Technical Administrator will have permissions to perform approve or reject actions on a service requisition that needs approval. Every requisition that needs approval waits in the queue until it is either approved or rejected. Performer of the approvals will be notified whenever a requisition that needs approval enters the approval queue.

When a requisition is rejected, email notification will be sent out to the requester of the service. No notification will be sent out when a requisition is approved.

Approvals needed by the Cloud Provider Technical Administrator will go into the queue created by default for the Cloud Provider Organization. Approvals needed by Organization Technical Administrator will go into organization-specific queues. These are the naming convention for the queues:

| Organization                | Queue                                 |
|-----------------------------|---------------------------------------|
| Cloud Provider Organization | Cloud Service Approval Administration |
| Other                       | Approvals for <Organization Name>     |

Approvals are mandatory for the following services and are automatically enabled:

| Service                    | Cloud Provider Administrator Approval is Required | Organization Administrator Approval is Required |
|----------------------------|---------------------------------------------------|-------------------------------------------------|
| Create Virtual Data Center | Yes                                               | No                                              |
| Add Network to VDC         | Yes                                               | No                                              |

- 
- Step 1** Choose **My Workspace** from the module drop-down list and click the **System Setup** tab.
- Step 2** On the System Setup portal, click the **Approvals** tab, then click **Configure Approvals** to open the form.



Figure 6-12 Configure Approvals

**Configure Approvals**  
Manage which services require approvals by administrators before being delivered.

Service Name: ...

Cloud Provider Administrator Approval:  Yes  No

Organization Administrator Approval:  Yes  No

Submit Order Reset

**Step 3** For each service, specify the following information:

| Field                                 | Action                                      |
|---------------------------------------|---------------------------------------------|
| Service Name                          | Select the service from the drop-down list. |
| Cloud Provider Administrator Approval | Select Yes or No                            |
| Organization Administrator Approval   | Select Yes or No.                           |

**Step 4** Click **Submit Order** and proceed to [Chapter 5, “Running the Configuration Wizard.”](#)





# CHAPTER 7

## Setting Up the Cloud Infrastructure

---



Note

If you used the Intelligent Automation for Cloud Quick Setup Wizard, you have already completed the tasks in this chapter. Skip to [Chapter 8, “Post-Configuration Options”](#) for optional configurations, or to [Chapter 9, “Setting Up an Organization and Adding Users”](#) to resume required configuration.

---



Note

Before you can perform the tasks in this chapter, you **MUST** complete **all** of the tasks, in sequence, that are presented in the previous chapters. You cannot proceed unless you have set up the Cloud Administrator organization and added Cloud Administrators.

---

You must now set up your cloud environment with data. This chapter provides instructions for setting up your cloud environment. It includes the following sections:

- [Connect the Cloud Platform Elements](#)
- [Set Provisioning Settings](#)
- [Set System-wide Service Options](#)
- [Stop and Start CIM Agents](#)
- [Remediating a Platform Element Discovery Error](#)
- [Create One or More PODs](#)
- [Register a Datastore](#)
- [Set Up a Shared Zone](#)



Note

Complete every task this chapter exactly as instructed and in the sequence that is presented. **Do not skip sections.**

---

# Connect the Cloud Platform Elements

You must first define the connection information for the platform elements that will be used in Cisco Intelligent Automation for Cloud 3.1.

In this section, you will define the connections for the following platform elements:

- Network Services Manager
- VMware vCenter Server
- Cisco UCS Manager
- Cisco Server Provisioner

These platform elements are associated with a Compute Point of Delivery (POD).

As you define each platform element, the discovery process automatically begins and runs in the background. If there is a discovery error for the platform element, you will receive an email notification.



## Note

Notifications of discovery errors will be set to the notifications email address for the Cloud Service Approval Administration queue. Instructions for assigning queue notifications appear in the previous chapter. If you have not done so, return to [Assign Mail Addresses for Queue Notifications, page 6-10](#), for instructions before you proceed with the tasks in this section.

## Define the VMware vCenter Server Platform Element

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

- Step 1** Open Cisco Cloud Portal and log in as a Cloud Provider Technical Administrator.
- Step 2** Choose **My Workspace** from the module drop-down list and click the **System Setup** tab.
- Step 3** On the System Setup portal, click the **Connections** tab to open the portlet.
- Step 4** On the Connections portlet, click **Connect Cloud Infrastructure** to open the form.

**Figure 7-1** Connect Cloud Infrastructure Form

- Step 5** On the Connect Cloud Infrastructure form, choose **VMware vCenter Server** from the Platform Element Type drop-down list.

**Caution**

**For Cisco IAC, vCenter object names cannot contain forward slashes.** If any of your vCenter object names contains forward slashes, please rename the files before you specify a vCenter path. For more information, please see the [VMware Software Preparation, page 1-9](#).

**Note**

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

- Step 6** Specify the following connection information for the VMware vCenter Server:

| Field                               | Action                                                                                                                                                                  |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name                           | Enter the IP address or the name of the server that hosts the VMware vCenter Server. For example: <i>test-esxvc-01.domain.local</i>                                     |
| Port                                | Enter the TCP/IP port used to connect to the VMware vCenter Server. By default, port 443 is used.                                                                       |
| Description                         | <i>Optional.</i> Enter information that describes the VMware vCenter server.                                                                                            |
| Secure Connection Protocol          | Click the <b>True</b> or <b>False</b> radio button to indicate whether secure connection protocol is used to connect to the server. <b>True</b> is selected by default. |
| User Name                           | Enter the account name to use when connecting to the VMware vCenter Server.                                                                                             |
| Enter password<br>Re-enter password | Enter and re-enter the password assigned to the account used to connect to the VMware vCenter Server.                                                                   |

- Step 7** Click **Submit Order**.

- Step 8** Keep the Connections portlet open and proceed to [Define the Cisco UCS Manager Platform Element](#). If you receive an email notification that discovery of the VMware vCenter platform element failed, proceed to the next sections to define the Cisco UCS Manager and Cisco Server Provisioner platform elements. When you have completed these tasks, see [Remediating a Platform Element Discovery Error, page 7-10](#), for instructions on how to remediate the error.

## Define the Cisco UCS Manager Platform Element

**Note**

You must be logged in as the Cloud Provider Technical Administrator to perform this task.

Complete the following steps to define the connection information for the Cisco UCS Manager that will be used in Intelligent Automation for Cloud 3.1.

- Step 1** On the Connections portlet, click **Connect Cloud Infrastructure** to open the form ([Figure 7-1 on page 7-2](#)).
- Step 2** On the Connect Cloud Infrastructure form, choose **Cisco UCS Manager** from the Platform Element Type drop-down list.



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

**Step 3** Specify the following connection information for the Cisco UCS Manager server:

| Field                      | Action                                                                                                                                                                                                                           |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name                  | Enter the host name or IP address for the Cisco UCS Manager server.<br>For example: test-ucs-000.domain.local                                                                                                                    |
| Port                       | Enter the TCP/IP port used to connect to the Cisco UCS Manager server.<br>By default, the following ports are used: <ul style="list-style-type: none"> <li>• Port 443—SSL protocol</li> <li>• Port 80—HTTP connection</li> </ul> |
| Description                | <i>Optional.</i> Enter information that describes the Cisco UCS Manager server.                                                                                                                                                  |
| Secure Connection Protocol | Click the <b>True</b> or <b>False</b> radio button to indicate whether secure connection protocol is used to connect to the server. True is selected by default.                                                                 |
| Ignore Certificate Error   | Click the <b>True</b> or <b>False</b> radio button to indicate whether certificate error messages should be ignored. <b>True</b> is selected by default.                                                                         |
| Time Zone                  | Choose the time zone that is used on the Cisco UCS Manager server from the drop-down list.                                                                                                                                       |
| User Name                  | Enter the account name to use when connecting to the Cisco UCS Manager server.                                                                                                                                                   |
| Enter password             | Enter the password assigned to the account used to connect to the Cisco UCS Manager server.                                                                                                                                      |
| Re-enter password          | Re-enter the password to confirm it.                                                                                                                                                                                             |

**Step 4** Click **Submit Order**.

**Step 5** Keep the Connections portlet open and proceed to [Define the Cisco Server Provisioner Platform Element](#).

If you receive an email notification that discovery of the Cisco UCS Manager platform element failed, proceed to the next section to define the Cisco Server Provisioner platform element, then see [Remediating a Platform Element Discovery Error, page 7-10](#), for instructions on how to remediate the error.

## Define the Cisco Server Provisioner Platform Element



**Note** You must be logged in as the Cloud Provider Technical Administrator to perform this task.

Complete the following steps to define the connection information for the Cisco Server Provisioner that will be used in Intelligent Automation for Cloud 3.1.

- Step 1** On the Connections portlet, click **Connect Cloud Infrastructure** to open the form ([Figure 7-1 on page 7-2](#)).
- Step 2** On the Connect Cloud Infrastructure form, choose **Cisco Server Provisioner** from the Platform Element Type drop-down list.



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

- Step 3** Specify the following connection information for the Cisco Server Provisioner server:

| Field             | Action                                                                                                                            |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Host Name         | Enter the host name or IP address for the Cisco Server Provisioner server.<br>For example: <i>test-sp-01.domain.local</i>         |
| Port              | Enter the TCP/IP port used to connect to the Cisco Server Provisioner server.<br>By default, Port 80 is used for HTTP connection. |
| Description       | <i>Optional.</i> Enter information that describes the Cisco Server Provisioner server.                                            |
| User Name         | <i>Read-only.</i> Defaults to the console root username of the Cisco Server Provisioner.                                          |
| Enter password    | <i>Read-only.</i> Defaults to the console root password of the Cisco Server Provisioner.                                          |
| Re-enter password | Re-enter the password to confirm it.                                                                                              |

- Step 4** Click **Submit Order**.
- If you receive an email notification that discovery of the Cisco Server Provisioner platform element failed, see [Remediating a Platform Element Discovery Error, page 7-10](#), for instructions on how to remediate the error.
- After remediating the error, proceed to [Set Provisioning Settings, page 7-6](#).

# Set Provisioning Settings

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



**Note** Setting provisioning settings automatically sets CIM File agent properties.

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

**Step 2** On the System Setup portal, click the **System Settings** tab.

**Step 3** On the System Settings portlet, click **Set Provisioning Settings**.



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


**Step 4** On the Server Provisioning Settings form, specify the following information:

| Field                                                          | Action                                                                                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Default Cisco Server Provisioner Time Zone                     | Set the default the time zone for Cisco Server Provisioner.                                                                                                                                                                                                                                                                                                    |
| Default VMware vCenter Clone Timeout (Minutes)                 | Enter the period of time allowed, specified in minutes, before a virtual machine deployment operation is determined as failed.                                                                                                                                                                                                                                 |
| Duplicate Alert Suppression Time period (Hours)                | Enter the amount of time, in whole hours, to suppress duplicate alerts related to cloud automation.                                                                                                                                                                                                                                                            |
| CloudSync Discovery Interval (Hours)                           | The amount of time, in whole hours, between consecutive periodical executions of the CloudSync infrastructure discovery service.                                                                                                                                                                                                                               |
| Cloud Domain                                                   | Enter the name of the Windows domain for commissioned Windows servers to join.                                                                                                                                                                                                                                                                                 |
| Cloud Domain User<br>Cloud Domain Password                     | Enter the username and password for the Windows domain user to join the Windows VM to the Windows domain.                                                                                                                                                                                                                                                      |
| Cloud Default Time Zone Linux                                  | <i>Linux only.</i> Choose the default time zone for the Linux server from the drop-down list. <sup>1</sup>                                                                                                                                                                                                                                                     |
| Cloud Default Time Zone Windows                                | <i>Windows only.</i> Choose the default time zone for the Windows server from the drop-down list. <sup>1</sup>                                                                                                                                                                                                                                                 |
| Cisco Cloud Portal Data Synchronization Dropbox Base Directory | Enter the name of the base directory for the Data Synchronization Dropbox. This directory is the parent directory for the Cisco Cloud Portal Input, Backup, and Temp directory locations.<br><br>This value should be specified as a UNC path or SFTP (Linux) path where TEO will create files for import by the Cisco Cloud Portal service item import agent. |
| Cisco Cloud Portal Drop Input Location                         | Enter the name of the input folder that you created for the Data Synchronization Dropbox. (See <a href="#">Create a Dropbox for Data Synchronization</a> , page 4-3.)                                                                                                                                                                                          |



| Field                                                | Action                                                                                                                                                                    |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco Cloud Portal Drop Backup Location <sup>2</sup> | Enter the name of the backup folder that you created for the Data Synchronization Dropbox. (See <a href="#">Create a Dropbox for Data Synchronization, page 4-3.</a> )    |
| Cisco Cloud Portal Drop Temp Location                | Enter the name of the temporary folder that you created for the Data Synchronization Dropbox. (See <a href="#">Create a Dropbox for Data Synchronization, page 4-3.</a> ) |

1. For valid time zone values, *see* the [VMware documentation](#) on VMware.com.

- Step 5** Click **Submit Order** to submit the form and display the Order Confirmation page for the service that you ordered. **Do not close the order confirmation.**
- Step 6** In the Requisition Details pane on the Order Confirmation page ([Figure 6-6 on page 6-8](#)), click the requisition number to open the requisition summary page.
- Step 7** Click **Comments & History** in the menu on the right side of the window.
- Step 8** In the System History pane on the Comments and History page, look for errors. If the dropbox settings are configured correctly, you will see a message that the CIM agents are updated successfully.
- Step 9** Close the Comments and History window.
- Step 10** Stop and restart the file adapter agents:
- Choose **Service Link** from the module drop-down list and click the **Control Agents** tab.
  - Press Shift and click the green icons  in the first column for **CIM File Import - Service Item** and **CIMFileUpdater-IPAddress**.
  - Click **Stop Selected**, then click **Yes** in the confirmation dialog box.  
Keep the two agents selected.
  - Click **Start Selected**, then click **Yes** in the confirmation dialog box.
- Step 11** Proceed to [Set System-wide Service Options](#).

## Set System-wide Service Options

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

- Order a VM from template
- Order a VM and install an operating system
- Order a physical server
- Create a virtual datacenter
- ESXi provisioning
- Shared zones

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

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

**Table 7-1 Prerequisite Configuration Steps**

| Step                                       | Requirement                                                                                                                                                                                                                                                                                                                                                            | Configuration Steps                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Create a virtual datacenter                | <ul style="list-style-type: none"> <li>vCenter platform element is registered</li> <li>POD is created</li> </ul>                                                                                                                                                                                                                                                       | <ul style="list-style-type: none"> <li>Register Datastores (<a href="#">page 7-12</a>)</li> <li>Create networks (<a href="#">page 8-21</a>)</li> </ul>                                                                                                                                                                                                                                                 |
| Shared zones                               | <ul style="list-style-type: none"> <li>vCenter platform element is registered</li> <li>POD is created</li> </ul>                                                                                                                                                                                                                                                       | <ul style="list-style-type: none"> <li>Register Datastores (<a href="#">page 7-12</a>)</li> <li>Create networks (<a href="#">page 8-21</a>)</li> </ul>                                                                                                                                                                                                                                                 |
| Order VM from Template                     | <ul style="list-style-type: none"> <li>VM templates created and discovered</li> <li>Virtual Data Center or Shared Zone is created</li> </ul>                                                                                                                                                                                                                           | <ul style="list-style-type: none"> <li>Register Virtual Machine templates (<a href="#">page 8-1</a>)</li> </ul>                                                                                                                                                                                                                                                                                        |
| Order a VM and install an operating system | <ul style="list-style-type: none"> <li>VLAN for Cisco Server Provisioner to use as its private PXE VLAN defined in vCenter</li> <li>Cisco Server Provisioner Operating System Template is created</li> <li>Virtual Data Center or Shared Zone is created</li> </ul>                                                                                                    | <ul style="list-style-type: none"> <li>Register Cisco Server Provisioner Platform Element (<a href="#">page 7-5</a>)</li> <li>Create/Modify POD to contain the Cisco Server Provisioner Platform Element</li> <li>Discover and Register Cisco Server Provisioner operating system templates (<a href="#">page 8-2</a>)</li> </ul>                                                                      |
| Order a physical server                    | <ul style="list-style-type: none"> <li>VLAN for Cisco Server Provisioner to use as its private PXE VLAN defined in UCS Manager</li> <li>At least one UCS service profile template for physical server provisioning is created</li> <li>Cisco Server Provisioner Operating System Template is created</li> <li>Virtual Data Center or Shared Zone is created</li> </ul> | <ul style="list-style-type: none"> <li>Place blades in the Physical Blade Pool (<a href="#">page 8-5</a>)</li> <li>Discover and register Cisco Server Provisioner operating system templates (<a href="#">page 8-2</a>)</li> <li>Discover and register Cisco UCS service profile templates (<a href="#">page 8-3</a>)</li> </ul>                                                                       |
| ESXi provisioning                          | <ul style="list-style-type: none"> <li>VLAN for Cisco Server Provisioner to use as its private PXE VLAN defined in UCS Manager</li> <li>At least one hypervisor UCS service profile template for each vCenter cluster is created</li> <li>Cisco Server Provisioner Operating System Template for ESXi is created</li> </ul>                                            | <ul style="list-style-type: none"> <li>Infrastructure Network is created (<a href="#">page 8-21</a>)</li> <li>Place blades in the Virtual Blade Pool (<a href="#">page 8-5</a>)</li> <li>Discover and register Cisco UCS service profile templates (<a href="#">page 8-3</a>)</li> <li>Discover and register Cisco Server Provisioner operating system templates (<a href="#">page 8-2</a>)</li> </ul> |

When a service is disabled, users (Organization Technical Administrators and Server Owners) are prevented from ordering from the portal or portlet, and from submitting service forms from the My Services module. Although users can see the portal or portlet of the disabled service, a “disabled” message displays, and “Submit” buttons are hidden on the service forms.

Disabling an option only affects what clients can order from the catalog from the time the Set System Wide Service Options service order is fulfilled. It does not affect current, active services that have already been ordered.

You can reenable a disabled service at any time.

- Step 1** In My Workspace, click the **Offer Management** tab, then click **Set System Wide Service Options** to open the form.

**Figure 7-2** Set System Wide Service Options Form

- Step 2** Disable a service by clicking the **No** radio button, or reenable a disabled service by clicking the **Yes** radio button.

- Step 3** *Optional.* Edit the customer message.



**Note** Because this message appears globally for all disabled services, it is recommended that you keep the description generic.

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

- Step 5 Close the order confirmation, and proceed to [Stop and Start CIM Agents](#).
- 

## Stop and Start CIM Agents

Stop and start the following agent:

- CIM File Import - Service Item
- 

- Step 1 Choose **Service Link** from the module drop-down list, then click the **Control Agents** tab to open the portal.  
The Control Agents portal displays a list of all agents.
- Step 2 While pressing and holding **Shift**, click the red icons ● next to **CIM File Import - Service Item**, then click **Start Selected**.  
The red icons turn to green, indicating that they are now sending and receiving.
- Step 3 Proceed to [Remediating a Platform Element Discovery Error](#).
- 

## Remediating a Platform Element Discovery Error

If you have received an email notification of a discovery error related to a platform element you defined, follow the instructions in this section to remediate the error.



### Note

If you have *not* received an error notification, skip this section and proceed to [Set Provisioning Settings, page 7-6](#).

---

- Step 1 In My Workspace, click the **Cloud Service Errors** tab.
- Step 2 In the grid on the Cloud Service Errors portal, locate the error and click it to highlight it.  
Error details appear in the Take Action area below the grid.
- Step 3 In the Take Action area, click one of the following:
- **Cancel**—(Always available) Halt the service immediately and take no further action. No cleanup or verification of the integrity of data is performed.
  - **Restart**—Performs a full rollback of all changes and restarts service fulfillment at the beginning.
  - **Retry**—Attempts to resume service fulfillment at the step that failed.
  - **Ignore**—Attempts to resume service fulfillment, skipping the step that failed.
  - **Rollback**—Relinquishes all resources, all infrastructure and service item changes are reversed, and restores the cloud to the state prior to the service fulfillment request.
- Step 4 Proceed to [Create One or More PODs](#).
-

# Create One or More PODs

Use the Create POD service to register an installed POD (Point Of Delivery) and select the instances that manage its resources, so that you can start using it in the cloud.



**Note** You must be logged in as a Cloud Provider Technical Administrator to create a POD.

- 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 **PODs** tab.
- Step 3** Click **Register a POD**.
- Step 4** On the POD Details form, define the platform elements:

**Table 7-1** POD Details

| Field                             | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name<br>Description               | Assign a name and description.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| VMware vCenter Instance           | This field is not editable; only one vCenter is allowed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| VMware Datacenter                 | Select the datacenter that is to serve this POD. There is a 1-to-1 mapping between datacenters and PODs.<br><br>If the drop-down list is empty, all available datacenters have been associated with a POD. For information about defining a new VMware datacenter, see <a href="#">Define the VMware vCenter Server Platform Element, page 7-2</a> .                                                                                                                                                                                                                                                                                                      |
| Cisco UCS Manager Instance        | <i>Optional.</i> Select the UCS Manager that is to serve this POD. There is a 1-to-1 mapping between UCS Managers and PODs.<br><br>If the drop-down list is empty, all available UCS Managers have been associated with a POD. For information about defining a new UCS Manager, see <a href="#">Define the Cisco UCS Manager Platform Element, page 7-3</a> .                                                                                                                                                                                                                                                                                            |
| Cisco Server Provisioner Instance | <i>Optional.</i> Select the Server Provisioner instance that is to serve this POD. A CSP can be associated with multiple PODs. This option requires: <ul style="list-style-type: none"> <li>vCenter Port Group for OS Provisioning - The port group inside the vCenter that will be used for the provisioning VLAN for bare metal installations.</li> <li>UCS VLAN for OS Provisioning - The VLAN associated with UCS that is used by the Server Provisioner for bare metal installations.</li> </ul> For information about defining a new Cisco Server Provisioner, see <a href="#">Define the Cisco Server Provisioner Platform Element, page 7-5</a> . |

- Step 5** Click **Submit Order** and proceed to [Register a Datastore](#)

# Register a Datastore

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

- Step 1** Choose **My Workspace** from the module drop-down list and click the **Manage Cloud Infrastructure** tab.
- Step 2** Select **Datastores** in the VMware vCenter resources. Discovered datastores for the VMware vCenter will be shown.

**Figure 7-3** Discovered Datastores

| Datastore Name             | Status      | vCenter Name                | Datacenter            | Datastore Path                          | First Discovered | Last Status Ch.  |
|----------------------------|-------------|-----------------------------|-----------------------|-----------------------------------------|------------------|------------------|
| ISO SHARE (READ ONLY)      | Discovered  | sp-41esxc-02 sbalsoft local | QAC ONLY (DO NOT USE) | QAC ONLY (DO NOT USE)/ISO SHARE (RE...  | 10/6/12 09:45... | 10/3/12 12:03... |
| is-ucs-400-20A-02          | Discovered  | sp-41esxc-02 sbalsoft local | QAC ONLY (DO NOT USE) | QAC ONLY (DO NOT USE)/is-ucs-400-20A... | 10/6/12 09:45... | 10/3/12 12:03... |
| is-ucs-400-20A-02          | Maintenance | sp-41esxc-02 sbalsoft local | QAC ONLY (DO NOT USE) | QAC ONLY (DO NOT USE)/is-ucs-400-20A... | 10/6/12 09:45... | 10/3/12 12:03... |
| SJC-ACS-205-TEST-CLRN1     | Discovered  | sp-41esxc-02 sbalsoft local | QAC ONLY (DO NOT USE) | QAC ONLY (DO NOT USE)/SJC-205-T...      | 10/6/12 09:45... | 10/3/12 12:03... |
| SJC-ACS-205-TEST-CLRN2     | Registered  | sp-41esxc-02 sbalsoft local | QAC ONLY (DO NOT USE) | QAC ONLY (DO NOT USE)/SJC-205-T...      | 10/6/12 09:45... | 10/3/12 12:03... |
| is-ucs-401-primary         | Registered  | sp-41esxc-02 sbalsoft local | QAC ONLY (DO NOT USE) | QAC ONLY (DO NOT USE)/is-ucs-401-pr...  | 10/6/12 09:45... | 10/3/12 12:03... |
| SJC-ACS-205-TEST-CLRN3     | Discovered  | sp-41esxc-02 sbalsoft local | QAC ONLY (DO NOT USE) | QAC ONLY (DO NOT USE)/SJC-205-T...      | 10/6/12 09:45... | 10/3/12 12:03... |
| 41esxc-02-40-DOCK-FLUSE    | Discovered  | sp-41esxc-02 sbalsoft local | ESX-41                | ESX-41/41esxc-02-40-DOCK-FLUSE          | 10/6/12 09:45... | 10/3/12 12:03... |
| 41esxc-02-40-DOCK-FLUSE    | Discovered  | sp-41esxc-02 sbalsoft local | ESX-41                | ESX-41/41esxc-02-40-DOCK-FLUSE          | 10/6/12 09:45... | 10/3/12 12:03... |
| sp-41esxc-shared-storage-1 | Discovered  | sp-41esxc-02 sbalsoft local | ESX-41                | ESX-41/sp-41esxc-shared-storage-1       | 10/6/12 09:45... | 10/3/12 12:03... |

- Step 3** Select a datastore with a status of Discovered that should be registered for use.
- Step 4** Click **Register**. This starts the Register Datastore service.
- Step 5** Enter a display name and description for the Datastore (optional).
- Step 6** Click **Submit Order** and proceed to **Set Up a Shared Zone**.

## Set Up a Shared Zone

A shared zone is a community virtual data center that can be used by server owners in any organization to provision virtual and physical servers. A shared zone community virtual data center lives on a cluster in a POD and has datastores, resource pools, and community networks resources associated with it. Multiple shared zones can be created by the Cloud Provider for server owners to provision servers in.

A virtual data center has an associated size that determines limits for the number of virtual servers, physical servers, vCPUs, CPU MHz, storage, and memory. Limits are enforced by comparing the sum of the number of provisioned virtual and physical servers and the vCPUs, memory, and storage for a server size against the limits defined for the virtual data center size. A VMware resource pool is created for each virtual data center. This allows further control of resource utilization by defining CPU and memory limits, as well as CPU and memory reservations in the VMware resource pool.

To set up a shared zone:

- Step 1** Choose **My Workspace** from the module drop-down list and click the **System Setup** tab.
- Step 2** On the System Setup portal, click the **Shared Zones** tab to open the portlet.
- Step 3** Click **Create a Shared Zone**.
- Step 4** On the Create a Shared Zone form, specify the following information:

| Field                    | Action                                                                                                                                                                                                                                                                                 |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Shared Zone Name         | Enter a descriptive name for the shared zone. This name will be displayed when server owners select the virtual data center.                                                                                                                                                           |
| Description              |                                                                                                                                                                                                                                                                                        |
| Connection Type          | Indicates whether this shared zone is connected to Internet or enterprise internal network. Select <b>Internet-Connected</b> or <b>Enterprise-Connected</b> .                                                                                                                          |
| Size                     | Select the Size of the Shared Zone Community Virtual Data Center. The size determines the maximum limits for the number of virtual servers, maximum number of vCPUs, CPU MHz, memory, and storage. The sizes can be customized by <link to Add, Modify, or Delete a VDC Size Standard> |
| Maximum Snapshots per VM | Read-only field determined by the VDC size selected. 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 servers 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 used 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 the CPU Limit (MHz) limit defined for the VDC Size.                                                                                                                                        |

| Field                         | Action                                                                                                                                                                                                                                   |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.                                                                                              |
| Number of Networks            | A virtual data center can contain multiple networks. Select the number of networks for this the virtual data center. If more than one network is selected, additional Add Network sections will be shown on the form.                    |
| POD                           | POD is the Compute Point of Delivery where the virtual data center will be commissioned. The POD is defined in the <a href="#">Create One or More PODs, page 7-11</a> section                                                            |
| Datacenter                    | Read-only field that shows the VMware data center for the selected POD.                                                                                                                                                                  |
| Cluster                       | Select the cluster the virtual data center will be deployed on. A cluster can host multiple virtual data centers.                                                                                                                        |
| Datastore                     | Select the datastore for the virtual data center VM storage. A single datastore can be associated with multiple virtual data centers.                                                                                                    |
| Resource Pool Name            | Read-only field that shows the resource pool name to be created for the virtual data center. The resource pool name is based on the organization and virtual data center name.                                                           |
| CPU Shares                    | Read-only field that shows the CPU Shares for the resource pool. The default is normal.                                                                                                                                                  |
| CPU Limit (MHz)               | Read-only field that shows the CPU Limit in MHz for the resource pool. This is based on the VDC Size selected. This corresponds directly to the VMware resource pool CPU Limit.                                                          |
| 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 (GB)          | 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 (GB)       | 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.                             |
| Network Name                  | Only community networks can be used in Shared Zone Community Virtual Data Centers. Select the community network to be used for the shared zone community virtual data center.                                                            |



| Field                   | Action                                                                                                                                              |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| vCenter Network Path    | Read-only field that shows the vCenter Network Path for the selected network.                                                                       |
| UCS Network Description | Read-only field that shows the UCS Network Path for the selected network.                                                                           |
| Network Address         | Read-only field that shows the subnet address for the selected network.                                                                             |
| Management Network      | Optionally, a management network can be associated with a virtual data center. If desired, select a management network for the virtual data center. |

**Step 5** Click **Submit Order**.

**Step 6** Proceed to one of the following chapters:

- (Optional) If you want to configure additional templates, Cisco UCS blades, additional permissions, standards, and email templates, proceed to [Chapter 8, “Post-Configuration Options.”](#)
- If you choose not to configure additional templates, Cisco UCS blades, additional permissions, standards, and email templates, skip to [Chapter 9, “Setting Up an Organization and Adding Users”](#) to continue required configurations.





# CHAPTER 8

## Post-Configuration Options

---



Note

Before you can configure any of the optional settings presented in this chapter, you **MUST** complete **all** of the tasks, in sequence, that are presented in the previous chapters.

---

After you have performed the steps outlined in [Chapter 7, “Setting Up the Cloud Infrastructure,”](#) for configuring platform elements, provisioning, networks, and shared zone, you can then optionally perform any of the following tasks:

- [Managing Server Templates, page 8-1](#)
- [Manage Blade Pools, page 8-5](#)
- [Modify Standards for Service Options, page 8-7](#)
- [Add Additional Networks, page 8-21](#)
- [Inactivate Reserved Portlet Buttons from the My Workspace Toolbar, page 8-23](#)

## Managing Server Templates

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

- Virtual machine (VM) template
- Operating system (from Cisco Server Provisioner)
- UCS service profile template

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

## Registering a Virtual Machine Template

The Cloud Portal Technical Administrator can Register an existing virtual machine (VM) template in the cloud system for users to select when ordering virtual machines. The template may be in Discovered, Maintenance, or Ignored states to be changed to Registered. Register an existing virtual machine template in the cloud system for users to select when ordering virtual machines.



Note

Before you can register a VM template, it must first be defined in vCenter and discovered using the CloudSync Infrastructure Discovery portal.

---

To register a VM Template:

- Step 1 Choose **My Workspace** from the module drop-down list and then click **Manage Cloud Infrastructure**.
- Step 2 Click the **VM Templates** icon.

Figure 8-1 VM Templates Portlet

| VM Template Name                        | Status      | vCenter Name                   | Datacenter             | Full Path                                               | First Discover... | Last Status C... |
|-----------------------------------------|-------------|--------------------------------|------------------------|---------------------------------------------------------|-------------------|------------------|
| IAC Template - RHEL5 x64                | Registered  | sjc-41esxvc-02.tidalsoft.local | CIAC ONLY (DO NOT USE) | CIAC ONLY (DO NOT USE)/Templates/IAC Template - RHE...  | 10/11/12 02:3...  | 10/26/12 04:0... |
| IAC Template - Ubuntu12.04 x64          | Not Found   | sjc-41esxvc-02.tidalsoft.local | CIAC ONLY (DO NOT USE) | CIAC ONLY (DO NOT USE)/Templates/IAC Template - Ubu...  | 10/11/12 02:3...  | 10/16/12 12:0... |
| IAC Template - CentOS6 x64              | Discovered  | sjc-41esxvc-02.tidalsoft.local | CIAC ONLY (DO NOT USE) | CIAC ONLY (DO NOT USE)/Templates/IAC Template - Cen...  | 10/11/12 02:3...  | 10/26/12 04:0... |
| IAC Template - Windows 2008R2 x64       | Registered  | sjc-41esxvc-02.tidalsoft.local | CIAC ONLY (DO NOT USE) | CIAC ONLY (DO NOT USE)/Templates/IAC Template - Win...  | 10/11/12 02:3...  | 10/26/12 04:0... |
| IAC Template - Cisco Server Provisioner | Not Found   | sjc-41esxvc-02.tidalsoft.local | CIAC ONLY (DO NOT USE) | CIAC ONLY (DO NOT USE)/Templates/IAC Template - Cisc... | 10/11/12 02:3...  | 10/12/12 02:0... |
| IAC Template - CentOS5 x64              | Discovered  | sjc-41esxvc-02.tidalsoft.local | CIAC ONLY (DO NOT USE) | CIAC ONLY (DO NOT USE)/Templates/IAC Template - Cen...  | 10/11/12 02:3...  | 10/26/12 04:0... |
| VMW2K8R2STD_TEMPLATE                    | Maintenance | sjc-41esxvc-02.tidalsoft.local | ESX-41                 | ESX-41/VMW2K8R2STD_TEMPLATE                             | 10/11/12 02:3...  | 10/26/12 04:0... |
| Template-IAC-INT-RHEL                   | Maintenance | sjc-41esxvc-02.tidalsoft.local | ESX-41                 | ESX-41/Templates/Template-IAC-INT-RHEL                  | 10/11/12 02:3...  | 10/26/12 04:0... |
| Windows2008Ent                          | Discovered  | sjc-41esxvc-02.tidalsoft.local | ESX-41                 | ESX-41/Discovered virtual machine/Windows2008Ent        | 10/11/12 02:3...  | 10/26/12 04:0... |
| Template-IAC-INT-W2K8                   | Registered  | sjc-41esxvc-02.tidalsoft.local | ESX-41                 | ESX-41/Templates/Template-IAC-INT-W2K8                  | 10/11/12 02:3...  | 10/26/12 04:0... |

More Details:

- Display Name: **CentOS 6 64bit**
- Description: **IAC Template - CentOS6 x64**

- Step 3 Select the line item you wish to register in the grid, then select the **Register** button.
- Step 4 In **Register VM Template**, select the **Operating System Family**, then the **Operating System**.
- Step 5 Enter a friendly name in **Display Name**.
- Step 6 Enter a description in **Description**.
- Step 7 Click **Submit Order**.

## Registering an Operating System Template

The Cloud Portal Technical Administrator can Register an existing operating system template in the cloud system for users to select when ordering servers. The template may be in Discovered, Maintenance, or Ignored states to change it to Registered.



### Note

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

To register an operating system template:

- Step 1** Choose **My Workspace** from the module drop-down list and then click **Manage Cloud Infrastructure**.
- Step 2** Click the **OS Templates** icon.

**Figure 8-2** OS Templates Portlet

| OS Template Name                        | Status     | OS | OS Version        | Server        | First Discovered On | Last Status Check |
|-----------------------------------------|------------|----|-------------------|---------------|---------------------|-------------------|
| Test                                    | Discovered |    |                   | 10.201.76.151 | 10/18/12 01:58 PM   | 10/26/12 04:01 PM |
| CentOS 5.5 x86_64 Linux                 | Registered |    | CentOS 5/6 64-bit | 10.201.76.151 | 10/18/12 01:58 PM   | 10/26/12 04:01 PM |
| CentOS 6.0 x86_64 Linux                 | Registered |    | CentOS 5/6 64-bit | 10.201.76.151 | 10/18/12 01:58 PM   | 10/26/12 04:01 PM |
| ESXi 4.1.0                              | Registered |    | ESXi 4.1          | 10.201.76.151 | 10/18/12 01:58 PM   | 10/26/12 04:01 PM |
| Red Hat Enterprise Linux 5.1 i386       | Discovered |    |                   | 10.201.76.151 | 10/18/12 01:58 PM   | 10/26/12 04:01 PM |
| Ubuntu 10.04.0 i386 Server Linux        | Discovered |    |                   | 10.201.76.151 | 10/18/12 01:58 PM   | 10/26/12 04:01 PM |
| Windows Server 2008 R2 SERVERDATACENTER | Discovered |    |                   | 10.201.76.151 | 10/18/12 01:58 PM   | 10/26/12 04:01 PM |
| VMware ESXi 4.1 Hypervisor              | Registered |    | ESXi 4.1          | 172.21.45.35  | 10/22/12 06:54 PM   | 10/26/12 04:01 PM |
| Windows Server 2008 R2                  | Discovered |    |                   | 172.21.45.35  | 10/22/12 06:54 PM   | 10/26/12 04:01 PM |
| Red Hat Enterprise Linux 6 x86_64       | Discovered |    |                   | 172.21.45.35  | 10/22/12 06:54 PM   | 10/26/12 04:01 PM |

- Step 3** Select the line item you wish to register in the grid, and select the **Register** button.
- Step 4** In Register Operating System Template, select the **Operating System**.
- Step 5** Enter a friendly name in **Display Name**.
- Step 6** Enter a description in **Description**.
- Step 7** Click **Submit Order**.

## Registering a UCS Service Profile Template

The Cloud Portal Technical Administrator can Register an existing UCS service profile template in the cloud system for users to select when ordering servers. The template may be in Discovered, Maintenance, or Ignored states to change it to Registered.



### Note

Before you can register a UCS Service Profile Template, it must first be defined on the UCS Manager and discovered using the CloudSync Infrastructure Discovery portal.

To register a UCS service profile template:

- 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.

**Figure 8-3** Service Profile Templates Portlet

| Service Profile Template Name | Status     | UCS Manager                 | Full Path                                 | First Discovered ... | Last Status Check |
|-------------------------------|------------|-----------------------------|-------------------------------------------|----------------------|-------------------|
| David_T1                      | Discovered | sjc-ucs-200.tidalsoft.local | org-root/org-TEO_DevTestMs-David_T1       | 10/24/12 05:22 PM    | 10/26/12 04:01 PM |
| SE-ESX-TEMP                   | Discovered | sjc-ucs-200.tidalsoft.local | org-root/org-SE-ENV/Its-SE-ESX-TEMP       | 10/24/12 05:22 PM    | 10/26/12 04:01 PM |
| tsptest                       | Discovered | sjc-ucs-200.tidalsoft.local | org-root/Its-tsptest                      | 10/24/12 05:22 PM    | 10/26/12 04:01 PM |
| TEOCentOs                     | Discovered | sjc-ucs-200.tidalsoft.local | org-root/org-org-1/Its-TEOCentOs          | 10/24/12 05:22 PM    | 10/26/12 04:01 PM |
| TEOCentOs                     | Discovered | sjc-ucs-200.tidalsoft.local | org-root/Its-TEOCentOs                    | 10/24/12 05:22 PM    | 10/26/12 04:01 PM |
| TEOCentOS1                    | Discovered | sjc-ucs-200.tidalsoft.local | org-root/Its-TEOCentOS1                   | 10/24/12 05:22 PM    | 10/26/12 04:01 PM |
| DavidTemplate1                | Discovered | sjc-ucs-200.tidalsoft.local | org-root/org-TEO_DevTestMs-DavidTemplate1 | 10/24/12 05:22 PM    | 10/26/12 04:01 PM |
| kpmtest                       | Discovered | sjc-ucs-200.tidalsoft.local | org-root/Its-kpmtest                      | 10/24/12 05:22 PM    | 10/26/12 04:01 PM |
| QA-CSP-Test                   | Registered | sjc-ucs-200.tidalsoft.local | org-root/Its-QA-CSP-Test                  | 10/24/12 05:22 PM    | 10/26/12 04:01 PM |
| cc                            | Discovered | sjc-ucs-200.tidalsoft.local | org-root/org-Openstack/Its-cc             | 10/24/12 05:22 PM    | 10/26/12 04:01 PM |

- Step 3** Select the line item you wish to register in the grid, and select the **Register** button.
- Step 4** In Register Operating System Template, select whether this is a Hypervisor Template. If yes, select the **vCenter Cluster**.
- Step 5** Enter a friendly name in **Display Name**.
- Step 6** Enter a description in **Description**.
- Step 7** Click **Submit Order**.

# Manage Blade Pools

Use the Manage Blade Pools service to move UCS blades to and from physical and hypervisor pools, or to place blades into maintenance mode. This service enables you to control the balance of resource capacity allocated for each type of cloud activity.

- Step 1** Choose **My Workspace** from the module drop-down list and click the **System Setup** tab.
- Step 2** On the System Setup portal, click the **Blades and Pools** tab to open the portlet.
- Step 3** On the Blades & Pools portlet, click **Manage Blade Pools** to open the form.



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

- Step 4** On the Manage Blade Pools form, specify the following information:

| Field         | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UCS Manager   | <i>Display only.</i> The UCS Manager used for the cloud environment.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Chassis       | Choose the number of the UCS chassis where the blade is installed from the drop-down list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Blade         | Choose the number of the blade within the UCS chassis from the drop-down list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Resource Pool | <p><i>Display only.</i> Type of resource pool the blade is currently assigned.</p> <p>The following types of resource pools are available:</p> <ul style="list-style-type: none"> <li>Maintenance—Holding area for blades that have been registered but not identified for a specific purpose. These blades are owned and managed by the Cloud Administrator and are not available to Server Owners.</li> <li>Virtual—Includes blades that have been identified for hosting virtual servers and have been provisioned with ESXi.</li> </ul> <p><b>Note</b> Blades in this pool <i>never</i> carry a status of Available. The status will always be In Use or Pending.</p> <ul style="list-style-type: none"> <li>Physical—Includes blades that have been identified for use by Server Owners.</li> </ul> |

| Field             | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status            | <p><i>Display only.</i> Current availability status of the blade.</p> <p><b>Note</b> The blade must be <i>Available</i> to be commissioned for use or to move it to another resource pool.</p> <p>The following states may display:</p> <ul style="list-style-type: none"> <li>• Available—Unassigned and not currently in use; the blade is available for physical server provisioning or ESXi provisioning.</li> <li>• In Use—Assigned for use by either a Server Owner (running Windows or Linux) or assigned for use by the Cloud Administrator as an ESXi host.</li> <li>• Pending—Blade is in transition.</li> </ul> |
| New Resource Pool | Choose the resource pool to which the blade will be moved (Physical or Virtual) from the drop-down list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

**Step 5** Click **Submit Order**.

---



# Modify Standards for Service Options

Service option standards are the options that appear in drop-down lists for users to choose when ordering servers. Using the Standards service, you can control the available lease term options by adding or modifying of these service option standards.

This section provides instructions for the following tasks:

- [View Standards Settings, page 8-7](#)
- [Add, Modify, or Delete a Lease Term Standard, page 8-8](#)
- [Add, Modify, or Delete an Operating System Standard, page 8-11](#)
- [Add, Modify, or Delete a Server Size Standard, page 8-13](#)
- [Add, Modify, or Delete a VDC Size Standard, page 8-15](#)

You can add, modify, or delete the lease term, operating system, server, VDC or Shared Zone size standards for ordering servers. The values you set will appear as choices for users when ordering servers.

## View Standards Settings

View the default standard settings for lease term, operating systems, and server size to determine whether you want to change the values.

- 
- Step 1** Choose **My Workspace** from the module drop-down list, then click the **System Setup** tab.
  - Step 2** On the System Setup portal, click the **Standards** tab to open the portlet.
  - Step 3** On the Standards portlet, click **Define Order Standards**.
  - Step 4** In the Standard panel on the left, click **Lease Terms** in the Service Options folder on the left, and note the settings.



**Note** Lease term settings are defined in seconds. If you add or modify a lease term standard, you will need to know the number of seconds in the new lease duration. The table in [Step 7 of Add a New Lease Term Standard, page 8-8](#), lists seconds in hour and day units to help you calculate the values.

---

- Step 5** Repeat [Step 1](#) through [Step 4](#) for **OS Systems** and **Server Size**.
- 

To add, modify, or delete a standards, see the following sections:

- [Add, Modify, or Delete a Lease Term Standard](#)
- [Add, Modify, or Delete an Operating System Standard, page 8-11](#)
- [Add, Modify, or Delete a Server Size Standard, page 8-13](#)

## Add, Modify, or Delete a Lease Term Standard

Lease term standards define the lease duration options that users can choose from drop-down lists when they order servers.

A lease is a service option that sets a duration (for example, three months) on a server from the time it is commissioned. During the lease period, the server is active and accessible to users. When the lease term expires, the server is automatically decommissioned and placed into storage for a defined length of time. (When a server is decommissioned, it has not been deleted, but it is not accessible to users.) When the storage period expires, the server is deleted and its data is lost.

**Note**

A Server Owner can extend the lease on the server while it is active, or re-commission the server while it is in storage. Instructions for extending a lease and commissioning a server are provided in the [Cisco Intelligent Automation for Cloud 3.1 User Guide](#).

Each lease term standard has four settings:

- **Term**—The name of the option describing the duration of the lease. For example, 90 days. This value appears in the drop-down list for users to choose, so it must be clear and descriptive.
- **Runtime Seconds**—The duration of the lease, defined in seconds. The runtime value must always match the defined term. For example, a 30 day lease has a runtime value is 2592000 seconds. This value is hidden from users.

**Note**

The table in [Step 7 of Add a New Lease Term Standard, page 8-8](#), lists seconds in hour and day units to help you determine values for lease terms.

- **Storage Seconds**—The time period during which the server is stored after the lease expires. The default setting is 864000 seconds, or 10 days. This value is hidden from users.
- **Warning1Seconds**—The number of seconds before the lease expiration date when the first expiration warning notification is sent to the server owner. The default setting is 604800 seconds, or 7 days after commission. This value is hidden from users.
- **Warning2Seconds**—The number of seconds before the lease expiration date when the second expiration warning notification is sent to the server owner. The default setting is 86400 seconds, or 1 day before expiration. This value is hidden from users.

Cisco IAC ships with five pre-configured lease term standards: 30 days, 90 days, 6 months (180 days), 1 year, and No Lease. You can accept, modify, or delete a default lease term standard, and you can add a new standard.

This section provides instructions for the following modifications:

- [Add a New Lease Term Standard, page 8-8](#)
- [Modify a Lease Term Standard, page 8-10](#)
- [Delete a Lease Term Standard, page 8-11](#)

### Add a New Lease Term Standard

- Step 1** Choose **My Workspace** from the module drop-down list, then click the **System Setup** tab.
- Step 2** On the System Setup portal, click the **Standards** tab to open the portlet.

- Step 3** On the Standards portlet, click **Define Order Standards**.
- Step 4** Click **Lease Terms** in the Service Options folder on the left.
- Step 5** Click **Add New**. An empty row appears.
- Step 6** In the Standard Data table, click inside the Term field in the new row and enter a label for a unit of time (for example, 60 days). This entry will appear to users in the drop-down list on the order forms.



**Note** It is recommended that you avoid using months, because the numbers of days in months vary. Because lease durations are defined in seconds, and the seconds values would not be consistent from month to month. It is recommended that you use four-week units instead of months.

- Step 7** Click inside the Runtime Seconds field and enter the number of seconds in the Term duration you defined in [Step 5](#). Do not include commas in the value.

The Runtime Seconds value must match the Term you have entered. For example, the runtime value for a 60-day lease term is 5184000 seconds. Use the figures in the following table to calculate the Term duration in seconds.

| Duration                  | Runtime Value (Seconds) |
|---------------------------|-------------------------|
| 12 hours                  | 43200                   |
| 1 day                     | 86400                   |
| 7 days                    | 604800                  |
| 28 days                   | 2419200                 |
| 180 days (about 6 months) | 15552000                |
| 365 days (1 year)         | 31536000                |

- Step 8** In the Storage Seconds field, enter the amount of time, in seconds, during which the decommissioned server is held in storage. When this defined storage duration expires, the server will be deleted.



**Note** The suggested Storage Seconds value is 864000, or 10 days.

- Step 9** In the Warning1Seconds field, enter the amount of time, in seconds, before the lease expiration date when the first notification of expiration is automatically sent to the server owner.



**Note** The suggested Warning1Seconds value is 604800, or 7 days before lease expiration.

- Step 10** In the Warning2Seconds field, enter the amount of time, in seconds, before the lease expiration date when the second notification of expiration is automatically sent to the server owner.



**Note** Depending on the width of your screen, you may need to scroll to the right to see the Warning2Seconds field.



**Note** The suggested Warning2Seconds value is 86400, or 1 day before lease expiration.

Step 11 Click **Save**.

---

## Modify a Lease Term Standard



**Note** The Term label and the Runtime Seconds value **must** match. Do not modify either without modifying the other.

---

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

Step 2 On the System Setup portal, click the **Standards** tab.

Step 3 On the Standards portlet, click **Define Order Standards**.

Step 4 Click **Lease Terms** in the Service Options folder on the left.

Step 5 In the Standard Data column, click inside the Term field in the appropriate row and change the label (for example, 8 weeks). This entry will appear to users in the drop-down list on the order forms.



**Note** It is recommended that you avoid using months, because the numbers of days in months vary. Because lease durations are defined in seconds, and the seconds values would not be consistent from month to month. It is recommended that you use four-week units instead of months.

---

Step 6 Use the figures in the table [Step 7 of Add a New Lease Term Standard, page 8-8](#), to calculate a duration in seconds.



**Note** The runtime must match the number of seconds in the Term you have entered. Do not include commas in the value.

---

Step 7 For Storage Seconds, Warning1Seconds, and Warning2Seconds, you can change the values, or accept the default values:

- Storage Seconds—864000 (10 days)
- Warning1Seconds—604800 (7 days)
- Warning2Seconds—86400 (1 day)



**Note** Depending on the width of your screen, you may need to scroll to the right to see the Warning2Seconds field.

---

Step 8 Click **Save**.

---

## Delete a Lease Term Standard



**Note** Do not delete or modify the No Lease standard unless you want to enforce leases on servers. If you delete the No Lease standard, users will not be able order servers without leases.

- 
- Step 1** Choose **My Workspace** from the module drop-down list, then click the **System Setup** tab.
  - Step 2** On the System Setup portal, click the **Standards** tab to open the portlet.
  - Step 3** On the Standards portlet, click **Define Order Standards**.
  - Step 4** Click **Lease Terms** in the Service Options folder on the left.
  - Step 5** In the Standard Data column, click inside the Term field for the standard that you want to delete.
  - Step 6** Click **Delete**, then confirm the deletion.
  - Step 7** Click **Save**.
- 

## Add, Modify, or Delete an Operating System Standard

Cisco IAC ships with five pre-defined operating system standards that users can choose when commissioning virtual machines with operating systems installed and that administrators use to register VM templates:

- Linux—CentOS 5/6 64-bit
- Linux—Red Hat Enterprise Linux 6 64-bit
- Windows—Windows Server 2008 R2 64-bit
- VMware ESXi—ESXi 4.1
- ESXi—ESXi 5.0

You can accept or modify default operating system standards, and add new standards.

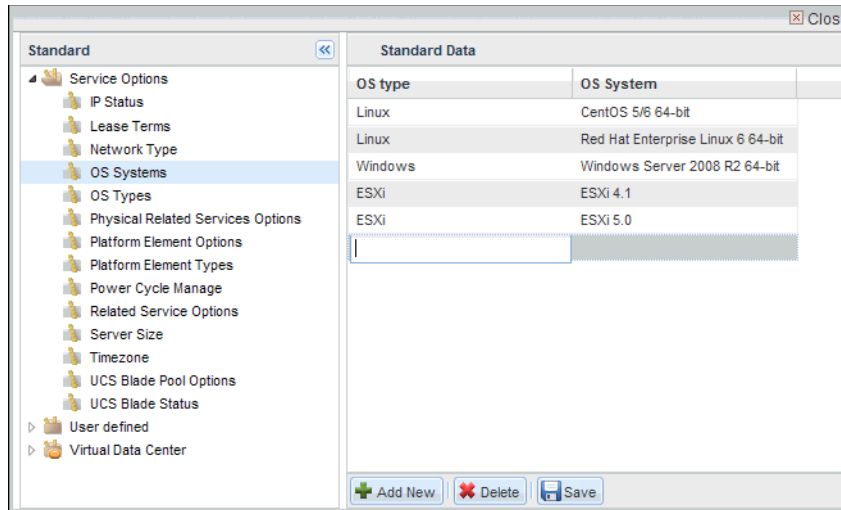
This section provides instructions for the following modifications:

- [Add an Operating System Standard, page 8-11](#)
- [Modify an Operating System Standard, page 8-12](#)
- [Delete an Operating System Standard, page 8-12](#)

## Add an Operating System Standard

- 
- Step 1** Choose **My Workspace** from the module drop-down list, then click the **System Setup** tab.
  - Step 2** On the System Setup portal, click the **Standards** tab.
  - Step 3** On the Standards portlet, click **Define Order Standards**.
  - Step 4** Click **OS Systems** in the Service Options folder on the left.
  - Step 5** Click **Add New**. An empty row appears.

Figure 8-4 Add a Standard—Operating Systems



- Step 6** In the Standard Data column, click inside the OS Type field in the new row and enter the OS Type (Windows, Linux, or VMware ESXi). This entry will appear to users in drop-down lists on the order forms.
- Step 7** In the OS System field, enter the name of the operating system and the version number.
- Step 8** Click **Save**.

## Modify an Operating System Standard

- Step 1** Choose **My Workspace** from the module drop-down list, then click the **System Setup** tab.
- Step 2** On the System Setup portal, click the **Standards** tab.
- Step 3** On the Standards portlet, click **Define Order Standards**.
- Step 4** Click **OS Systems** in the Service Options folder on the left.
- Step 5** In the Standard Data column, click inside the OS System field in the new row and edit the value.
- Step 6** Click **Save**.

## Delete an Operating System Standard

- Step 1** Choose **My Workspace** from the module drop-down list, then click the **System Setup** tab.
- Step 2** On the System Setup portal, click the **Standards** tab.
- Step 3** On the Standards portlet, click **Define Order Standards**.
- Step 4** Click **OS Systems** in the Service Options folder on the left.
- Step 5** In the Standard Data column, click inside the OS System field for the standard that you want to delete.
- Step 6** Click **Delete**, then confirm the deletion.

Step 7 Click **Save**.

---

## Add, Modify, or Delete a Server Size Standard

Cisco IAC ships with four pre-defined server size standards that users can choose when commissioning servers: Small, Medium, Large, and Extra Large. Each standard defines the CPU, Memory GB, and Storage GB, as shown in [Table 8-1](#).

*Table 8-1 Default Server Sizes*

| Server Size | CPUs | Memory (GB) | Storage (GB) |
|-------------|------|-------------|--------------|
| Extra Small | 1    | 1           | 30           |
| Small       | 2    | 2           | 30           |
| Medium      | 2    | 4           | 40           |
| Large       | 4    | 6           | 40           |
| Extra Large | 8    | 8           | 60           |

You can accept, modify, or delete a server size standard, and you can add a new standard.

This section provides instructions for the following modifications:

- [Add a Server Size Standard, page 8-13](#)
- [Modify a Server Size Standard, page 8-14](#)
- [Delete a Server Size Standard, page 8-14](#)

### Add a Server Size Standard

---

- Step 1 Choose **My Workspace** from the module drop-down list, then click the **System Setup** tab.
- Step 2 On the System Setup portal, click the **Standards** tab.
- Step 3 On the Standards portlet, click **Define Order Standards**.
- Step 4 Click **Server Size** in the Service Options folder on the left.
- Step 5 Click **Add New**. An empty row appears.

Figure 8-5 Add a Standard—Server Size

| Server Size | CPUs | Memory GB | Storage GB |
|-------------|------|-----------|------------|
| Small       | 2    | 2         | 20         |
| Medium      | 4    | 2         | 60         |
| Large       | 6    | 4         | 80         |
| Extra Large | 8    | 16        | 60         |
| Extra Small | 1    |           |            |

- Step 6** In the Standard Data column, click inside the Server Size field in the new row and enter the a label for the new size (for example, Extra Small). This entry will appear to users in drop-down lists on the order forms.
- Step 7** Enter the values for CPUs, Memory GB, and Storage GB in the appropriate fields.



**Note** Depending on the width of your screen, you may need to scroll to the right to see the Storage GB field.

- Step 8** Click **Save**.

## Modify a Server Size Standard

- Step 1** Choose **My Workspace** from the module drop-down list, then click the **System Setup** tab.
- Step 2** On the System Setup portal, click the **Standards** tab.
- Step 3** On the Standards portlet, click **Define Order Standards**.
- Step 4** Click **Server Size** in the Service Options folder on the left.
- Step 5** In the Standard Data table, click in any of the fields to set new values.
- Step 6** Click **Save**.

## Delete a Server Size Standard

- Step 1** Choose **My Workspace** from the module drop-down list, then click the **System Setup** tab.
- Step 2** On the System Setup portal, click the **Standards** tab.
- Step 3** On the Standards portlet, click **Define Order Standards**.



- Step 4** Click **Server Size** in the Service Options folder on the left.
- Step 5** In the Standard Data column, click inside the Server Size field for the standard that you want to delete.
- Step 6** Click **Delete**, then confirm the deletion.
- Step 7** Click **Save**.

## Add, Modify, or Delete a VDC Size Standard

Cisco IAC ships with six predefined VDC standards that OTAs can choose when commissioning VDCs:

- Small, Medium, and Large standards define the sizes for VDCs.
- Small Shared, Medium Shared, and Large Shared standards define the sizes for Shared Zones.

Each standard defines the following settings:

| Setting                                  | Description                                                                                                                                                                                                                                          |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maximum number of virtual servers limit  | The maximum number of virtual servers allowed in this VDC. After this limit has been reached, additional virtual servers cannot be created in the VDC.                                                                                               |
| Maximum number of vCPU limit             | The maximum number of vCPUs allowed in this VDC. After this limit has been reached, additional virtual servers cannot be created in the VDC.                                                                                                         |
| Maximum memory (GB) limit                | The maximum amount of memory in GB allowed in this VDC. Enforcement of this limit is based on the memory specification in the Server standards. The memory limit is also used for creating the VMware resource pool.                                 |
| Maximum total storage (GB) limit         | The maximum amount of memory in GB allowed in this VDC. Enforcement of this limit is based on the storage specification in the Server standards. It does not account for thin provisioning or space used by snapshots.                               |
| Maximum number of physical servers limit | The maximum number of virtual servers allowed in this VDC. After this limit has been reached, additional virtual servers cannot be created in the VDC.                                                                                               |
| CPU Limit (MHz)                          | The maximum amount of CPU in MHz virtual servers in this VDC is allowed to use. This number is determined by the CPU compute capacity available in the cluster. This is enforced through the VMware resource pool CPU Limit. -1 specifies unlimited. |
| Resource Pool CPU Reservation (MHz)      | The amount of CPU in MHz to reserve for this VDC. The reservation is handled by the VMware resource pool CPU Reservation. The default is 0.                                                                                                          |
| Resource Pool Memory Reservation (GB)    | The amount of memory in GB to reserve for this VDC. The reservation is handled by the VMware resource pool Memory Reservation. The default is 0.                                                                                                     |

| Setting                          | Description                                                                                                                                                                                                                                                 |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Number of Snapshots              | Default value for maximum number of snapshots allowed per VDC. After this limit has been reached for a virtual server, no additional snapshots can be taken for that server.                                                                                |
| Community VDC (Yes - No boolean) | Specifies whether this standard applies to a Shared Zone Community VDC. This should be set to <b>Yes</b> , if this standard is for a Shared Zone Community VDC and <b>No</b> , if this standard is for an organization VDC. This setting is case sensitive. |
| Size Order                       | Specifies the order of the sizes relative to each other. An Integer is used to define this. For example, Small is 1, Medium is 2, Large is 3.                                                                                                               |

The following table summarizes the maximum values for the virtual servers. You can accept, modify, or delete a server size standard, or you can add a new standard. To add a new standard, use the VDC Size Calculator determine the proper VDC sizing. For more information about the VDC Calculator, see [Planning VDC Package Sizing, page 8-18](#).

|               | Max Virtual Servers | Max vCPU | Max Memory (GB) | Max Total Storage (GB) | Max Physical Servers | CPU Limit (MHz) | Resource Pool CPU Reservation (MHz) | Resource Pool Memory Reservation (GB) | Number of Snapshots | Community VDC |
|---------------|---------------------|----------|-----------------|------------------------|----------------------|-----------------|-------------------------------------|---------------------------------------|---------------------|---------------|
| Small         | 50                  | 74       | 296             | 7500                   | 0                    | 22,200          | 0                                   | 0                                     | 5                   | No            |
| Medium        | 100                 | 145      | 580             | 14,750                 | 2                    | 43,500          | 0                                   | 0                                     | 5                   | No            |
| Large         | 250                 | 366      | 1458            | 37,002                 | 4                    | 109,200         | 0                                   | 0                                     | 5                   | No            |
| Small Shared  | 250                 | 366      | 1458            | 37,002                 | 10                   | 109,200         | 0                                   | 0                                     | 5                   | Yes           |
| Medium Shared | 500                 | 725      | 2900            | 73,750                 | 10                   | 217,500         | 0                                   | 0                                     | 5                   | Yes           |
| Large Shared  | 1000                | 1450     | 5800            | 147,500                | 10                   | 435,000         | 0                                   | 0                                     | 5                   | Yes           |

This section provides instructions for the following modifications:

- [Add a VDC Size Standard, page 8-16](#)
- [Modify an Operating System Standard, page 8-12](#)
- [Delete a VDC Size Standard, page 8-18](#)
- [Planning VDC Package Sizing, page 8-18](#)

## Add a VDC Size Standard

- Step 1** Use the VDC calculator to calculate the appropriate values for the number of virtual servers for this standard.
- Step 2** Choose **My Workspace** from the module drop-down list, then click the **System Setup** tab.

- Step 3 On the System Setup portal, click the **Standards** tab.
- Step 4 On the Standards portlet, click **Define Order Standards**.
- Step 5 Click **VDC Sizes** in the Virtual Data Center folder on the left.
- Step 6 Click **Add New**. An empty row appears.

Figure 8-6 Add a Standard—VDC Size

| Standard | Name          | Maximum number of virtual machines | Maximum number of vCPU s | Maximum memory (GB) limit | Maximum total storage (GB) L | Maximum number of hosts |
|----------|---------------|------------------------------------|--------------------------|---------------------------|------------------------------|-------------------------|
|          | Small Shared  | 250                                | 532                      | 8400                      | 1981355                      | 10                      |
|          | Small         | 50                                 | 108                      | 1720                      | 378000                       | 5                       |
|          | Medium Shared | 500                                | 1052                     | 16420                     | 3960500                      | 10                      |
|          | Medium        | 100                                | 211                      | 3364                      | 792100                       | 2                       |
|          | Large         | 250                                | 532                      | 8400                      | 1981355                      | 10                      |
|          | Large Shared  | 1000                               | 2103                     | 33640                     | 7921000                      | 10                      |
|          | Extra Small   | 25                                 |                          |                           |                              |                         |

- Step 7 In the Standard Data column, click inside the Name field in the new row and enter the a label for the new size (for example, Extra Small). This entry will appear to users in drop-down lists on the order forms.
- Step 8 Enter the values for the other fields based on the results provided by the VDC Size calculator.



**Note** Depending on the width of your screen, you may need to scroll to the right to see the Storage GB field.

- Step 9 Enter **Yes** if this standard is a shared zone community VDC or **No** if this standard is for a organization VDC.
- Step 10 For the Size Order, specify an integer for the new standards size relative to the other sizes. For example, 1 for Small, 2 for Medium, 3 for Large.
- Step 11 Click **Save**.

## Modify a VDC Size Standard

- Step 1 Choose **My Workspace** from the module drop-down list, then click the **System Setup** tab.
- Step 2 On the System Setup portal, click the **Standards** tab.
- Step 3 On the Standards portlet, click **Define Order Standards**.
- Step 4 Click **VDC Sizes** in the Virtual Data Center folder on the left.
- Step 5 In the Standard Data table, click in any of the fields to set new values.
- Step 6 Click **Save**.

## Delete a VDC Size Standard

- Step 1 Choose **My Workspace** from the module drop-down list, then click the **System Setup** tab.
- Step 2 On the System Setup portal, click the **Standards** tab.
- Step 3 On the Standards portlet, click **Define Order Standards**.
- Step 4 Click **VDC Sizes** in the Virtual Data Center folder on the left.
- Step 5 In the Standard Data table, click inside the Name field for the standard that you want to delete.
- Step 6 Click **Delete**, then confirm the deletion.
- Step 7 Click **Save**.

## Planning VDC Package Sizing



**Note**

Only Cloud Provider Technical Administrators have access to this feature.

Cloud Provider Technical Administrators often need to determine the most effective sizes for virtual data center packages to match their customer's needs. To avoid any big leftover gaps or unused resources, the VDC Calculator can help build well-balanced offerings that closely match a customer needs, with the correct ratios between size elements of the package (CPU, memory, and storage resource limitations).

- Step 1 Choose **My Workspace** from the module drop-down list and click the **VDC Calculator** tab. Then, in the Planned VDC VM Limit step, enter the approximate number of virtual machines in the VDC.

**Figure 8-7 VDC Calculator**

**VDC Calculator Steps**

1. Enter the total number of virtual machines in the Planned VDC VM Limit field.
2. Enter names for each VM size and respective virtual machine percentages for the planned VDC VM Limit.
3. Enter respective virtual machine configuration attributes for each size.
4. Displayed is the Suggested VDC Package size attributes.

**Step 1. Planned VDC VM Limit**

VDC VM Limit:

**Step 2. Planned VM Distribution**

**Step 3. Planned VM Configuration**

**Step 4. Suggested VDC Package**

**Step 2** In the **Planned VM Distribution** step, enter names for each virtual machine size and the respective virtual machine percentages. For readability, try to make the distribution percentage equal to 100%.

**Figure 8-8** *Planned VM Distribution*

Step 1. Planned VDC VM Limit

Step 2. Planned VM Distribution

|        |    |   |
|--------|----|---|
| Small  | 75 | % |
| Medium | 15 | % |
| Large  | 10 | % |

Step 3. Planned VM Configuration

Step 4. Suggested VDC Package

**Step 3** The **Planned VM Configuration** step displays the respective virtual machine configuration attributes for each size. The VDC Calculator uses these attributes, plus the following values, to create a weighted average:

- **MHz allocated per vCPU**—Enter how much real CPU (in MHz) should be assumed per vCPU allocated to a VM. This drives the total MHz boundaries of the resource pool.
- **Snapshots per VM**—Enter how many snapshots will be assumed when calculating the suggested datastore size.

**Figure 8-9** *Planned VM Configuration*

Step 1. Planned VDC VM Limit

Step 2. Planned VM Distribution

Step 3. Planned VM Configuration

|        | VM Quantity | vCPU Count | Memory (GB) | Storage (GB) | MHz allocated per vCPU | Snapshots per VM |
|--------|-------------|------------|-------------|--------------|------------------------|------------------|
| Small  | 75          | 1          | 4           | 40           |                        |                  |
| Medium | 15          | 2          | 8           | 60           | 300                    | 1.5              |
| Large  | 10          | 4          | 16          | 200          |                        |                  |

Step 4. Suggested VDC Package



**Step 4** The VDC Calculator returns the suggested VDC package.

**Figure 8-10 Suggested VDC Package**

Step 1. Planned VDC VM Limit

Step 2. Planned VM Distribution

Step 3. Planned VM Configuration

Step 4. Suggested VDC Package

Total vCPUs Total Memory (GB) Total Storage (GB) Total MHz  
145 580 14750 43500

Restore Defaults



# Add Additional Networks



**Note**

You must be logged in as a Cloud Provider Technical Administrator to add a network.

You can add the following types of networks:

- An infrastructure network

Infrastructure networks are used to deploy the management interfaces of the components which make up your cloud. Generally this represents the management network for VMware ESX hosts. Registration of at least one infrastructure network is required for ESXi hosts.

- A community network.

Community networks are available to any cloud user for deploying servers.

- A user network

Define a shared or controlled-access network within the cloud system for users in an organization to deploy servers. A user network can be dedicated to one organization or shared across organizations.

- A management network

A management network can optionally be assigned to a user network. A management network within the cloud system may be used to manage cloud servers, for example, for remote access and monitoring.

To add a network:

- Step 1** Open Cloud Portal and log in as a Cloud Provider Technical Administrator.
- Step 2** Choose **My Workspace** from the module drop-down list and click the **System Setup** tab.
- Step 3** On the System Setup portal, click the **Networks** tab to open the portlet, then click **Add a Network** to open the form.
- Step 4** On the Add Network form, specify the following information:



**Note**

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

| Field                        | Action                                                                                                                                                                            |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network Name                 | Enter a short network name that will be shown to users in the drop-down lists.                                                                                                    |
| Subnet Address Specification | Enter the network for this subnet in CIDR notation. Enter only an IPv4 type of IP address. For example, 192.168.1.x/24.<br><b>Note</b> The subnets from /23 to /29 are supported. |
| Community Network            | This setting is only available if the Network Type is User.                                                                                                                       |
| Public Network               | Specify the duplication policy for this network. Public networks are globally unique; private networks must only be unique within associated network device contexts.             |
| Network Type                 | Choose the network type from the drop-down list.<br>For Community networks, choose <b>User</b> .                                                                                  |

| Field             | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network Source    | Select how IP addresses management is done in this network: Internally by Cisco IAC, or via an external IP management tool.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| vCenter Portgroup | Select the vCenter portgroup that corresponds to the IP range being created.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| UCS VLAN          | Select the UCS VLAN that corresponds to the IP range being created. The UCS VLAN should match the VLAN for the vCenter portgroup.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Subnet Mask       | <i>Display only.</i> The subnet mask is generated from the prefix of the vCenter network you specified on this form.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Gateway Address   | <p>The “gateway” address is the floating “VIP” shared by the real members.</p> <p>Use the default gateway network that is populated from the subnet address or enter a different gateway network address (for example, 192.168.1.x).</p> <p><b>Note</b> The prepopulation of the gateway address is a convenience feature; if it doesn't suggest the address that is right for your network, you should either correct or remove it.</p> <p>This IP address will not be assigned to any server deployed by the system.</p>                                                                                                                                                               |
| FHRP1 Address     | <p>FHRP is a term used to describe the various First Hop Redundancy Protocols. This includes HSRP (common at Cisco) and VRRP (common outside of Cisco). The FHRP 1 and 2 address are the “real” IP addresses of the routers participating in the redundancy protocol.</p> <p>Enter the FHRP (First Hop Redundancy Protocol) gateway 1 and 2 network IP addresses, or keep the default values.</p> <p><b>Note</b> The prepopulation of the FHRP addresses are a convenience feature; if they don't suggest the address that is right for your network, you should either correct or remove them.</p> <p>These IP addresses will not be assigned to any server deployed by the system.</p> |
| FHRP2 Address     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Broadcast Address | Use the default broadcast address that is populated from the subnet address or enter a different broadcast network address. For example, 192.0.2.255. This IP address will not be assigned to any server deployed by the system.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |



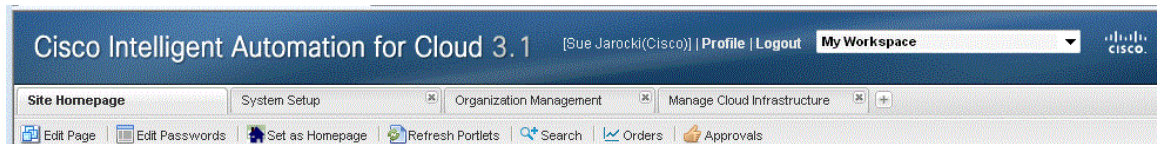
| Field         | Action                                                                                                                                                                                                                                                        |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Primary DNS   | Enter one of the following: <ul style="list-style-type: none"> <li>The valid primary DNS address for servers on this network</li> <li>A dummy primary DNS address.</li> </ul> This IP address will not be assigned to any server deployed by the system.      |
| Secondary DNS | Enter one of the following: <ul style="list-style-type: none"> <li>The valid secondary DNS address for servers on this network.</li> <li>A dummy secondary DNS address.</li> </ul> This IP address will not be assigned to any server deployed by the system. |

**Step 5** Click **Submit Order**, then proceed to [Inactivate Reserved Portlet Buttons from the My Workspace Toolbar](#).

## Inactivate 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 8-11** 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.

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

To inactivate the reserved portlets, complete the following steps.

- 
- 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**.

---



## CHAPTER 9

# Setting Up an Organization and Adding Users

---



Note

Before you can configure any of the optional settings presented in this chapter, you **MUST** complete **all** of the tasks presented in [Chapter 7, “Setting Up the Cloud Infrastructure.”](#)

---

This chapter guides you through setting up organizations and users. It includes the following sections:

- [Create an Organization](#)
- [Set Up Directory Integration \(If Applicable\)](#)
- [Create a New User to Add as an Organization Technical Administrator](#)
- [Add a Server Owner](#)
- [Assign Mail Addresses for Queue Notifications](#)



Note

Complete every task this chapter exactly as instructed and in the sequence that is presented. **Do not skip sections.**

---

## Create an Organization

Organizations in the Cisco IAC solution typically correspond to organizations company organizational structures such as Sales, Engineering, HR. Organizations must be created first before users can be added.

When an organization is created, an Approval Queue named 'Approvals for <org name>' is also created to handle approvals for that organization.

---

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

**Step 2** On the Organization Management portal, click **Create Organization** to open the form.




---

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

---

**Step 3** On the Create Organization form, specify the following information:

| Field                    | Action                                                                                                                                    |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Organization Name        | A descriptive name for the organization.                                                                                                  |
| Organization Description | <i>Optional.</i> Any relevant information about the organization that a user with organization management permissions would need to know. |

---

**Step 4** Click **Submit Order**, then proceed to [Set Up Directory Integration \(If Applicable\)](#).

---

## Set Up Directory Integration (If Applicable)




---

**Note** If you are not using a directory service for external authentication, skip to [Create a New User to Add as an Organization Technical Administrator](#).

---

If you will be using a directory service for external authentication, you do not need to perform any of the remaining tasks for creating users presented this final chapter. Proceed to [Appendix A “Setting Up Directory Integration.”](#)

After you have configured directory integration, your Cisco IAC setup is complete.

# Create a New User to Add as an Organization Technical Administrator

If you are not using a directory service, complete the following steps to assign an existing user as an Organization Technical Administrator for an organization.

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 add Server Owners, or users, within the organization (see [Add a Server Owner](#), page 9-4).



## Note

If the information shown in [Figure 9-1](#) appears on the Add Organization Technical Administrator form, it is strongly recommended that you do not proceed with the Add Organization Technical Administrator service. In this case, the external directory has already defined the user with an organization and role. Any changes you make will be overridden by the definitions set in the directory.

**Figure 9-1** Directory Authorization Notation

| Directory Integration                                                            |
|----------------------------------------------------------------------------------|
| Status: External authentication has been enabled                                 |
| Import Users: Accounts will be created from the directory                        |
| Role Assignment: User roles will be automatically assigned by directory mappings |

**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.



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

**Step 3** On the Add Organization Technical Administrator form, choose the organization to which you want to add the new user as an Organization Technical Administrator.

**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 user's first and last name.                         |
| Login                        | Enter a unique login identifier for the user.                 |
| Email                        | Enter the user's primary email address.                       |
| Time Zone                    | Choose the time zone of the user's primary physical location. |
| Password<br>Confirm Password | Create, then re-enter a password for the user.                |

- Step 6** Click **Submit Order**.
- Step 7** Proceed to [Add a Server Owner](#).

## Add a Server Owner

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

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

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

- Step 1** Choose **My Workspace** from the module drop-down list and click the **User Management** tab.
- Step 2** On the User Management portal, click **Add User** to open the form.
- Step 3** On the Add User form, choose the organization to which you want to add the new user as a Server Owner.
- Step 4** Choose **Create New User** from the Action drop-down list.



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

- Step 5** Provide the following information:

| Field                        | Action                                                                                                                                                                                                                                                                                            |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| First Name<br>Last Name      | Enter the first and last name of the new Server Owner.                                                                                                                                                                                                                                            |
| Login                        | Enter a unique login identifier for the new Server Owner.                                                                                                                                                                                                                                         |
| Email                        | Enter the new Server Owner's email address.                                                                                                                                                                                                                                                       |
| Roles                        | Click one of the following radio buttons to indicate the role to be assigned to the user: <ul style="list-style-type: none"> <li>• Virtual Server Owner—User can order virtual servers.</li> <li>• Virtual and Physical Server Owner—User can order both virtual and physical servers.</li> </ul> |
| Time Zone                    | From the drop-down list, choose the time zone associated with the new Server Owner's primary address.                                                                                                                                                                                             |
| Password<br>Confirm Password | Enter, then re-enter the password for the new Server Owner.                                                                                                                                                                                                                                       |

- Step 6** In the Roles field, click one of the following radio buttons to indicate the role to be assigned to the user:
- Virtual Server Owner—User can order virtual servers.
  - Virtual and Physical Server Owner—User can order both virtual and physical servers.

Step 7 Click **Submit Order**.

---

## Assign Mail Addresses for Queue Notifications

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

When an organization is created, Cisco IAC creates the following approvals queue:

Approval for <*Organization Name*>

This queue will contain tasks that are waiting for approval by the Organization Technical Administrator. Cloud Provider Technical Administrators and Organization Technical Administrators can monitor, assign, or address tasks added to the queues. Those users with access to the queues can perform the tasks added to the queues. When a task is added to a queue or is assigned or reassigned to a user, the designated users receive email notifications.



Note

For information about working with queues, see the [Cisco Intelligent Automation for Cloud 3.1 User Guide](#).

---

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



Tip

Use mailing lists (aliases), not specific user email addresses.

---



Note

You must configure email addresses for each queue.

---

To specify email addresses to queues, complete the following steps.

---

- Step 1 Log in to Cloud Portal as an Cloud Provider Technical administrator.
  - Step 2 Choose **Organization Designer** from the module drop-down list, then click the **Queues** tab.
  - Step 3 In the Queues pane, click **Approvals for <Organization Name>**.
  - Step 4 From the menu on the right side of the window, click **Contact** to display the Contact pane.
  - Step 5 Click **Add New** button, select email as the Type and enter the email address in the value field.
  - Step 6 Click **Update**.
-







# CHAPTER 10

## Upgrading to Cisco Intelligent Automation for Cloud 3.1

---

This chapter shows you how to upgrade from Cisco Intelligent Automation for Cloud (Cisco IAC) Starter Edition 3.0.2 on Cisco Cloud Portal 9.4 to Cisco Intelligent Automation for Cloud 3.1 on Cloud Portal 9.4. It provides full instructions for the installation using Microsoft SQL Server as the database server. Upgrades for CP running on Oracle are also supported.



### Note

---

Use the procedures in this document only when you are upgrading from an existing (working) IAC Starter Edition 3.0.2 system running on Cloud Portal 9.4.

---

This guide contains the following sections:

- [Upgrade Prerequisites](#)
- [Differences Between Cisco Intelligent Automation for Cloud Starter Edition and Cisco Intelligent Automation for Cloud 3.1](#)
- [Supported Upgrade Scenarios](#)
- [Actions Performed by the Upgrade Process](#)
- [Upgrade to Cisco Intelligent Automation for Cloud 3.1](#)

## Upgrade Prerequisites

- The environment has Cloud Portal 9.4 and Cisco IAC Starter Edition 3.0.2 deployed.
- Every Cisco IAC 3.1 organization must have a dedicated resource pool; a resource pool can only be used by one organization. If a resource pool is shared between organizations, then a new organization-specific resource pool must be created and virtual servers owned by organizations migrated to that resource pool.
- VSphere PowerCLI 5.0.1 is installed on the TEO Server.

## Differences Between Cisco Intelligent Automation for Cloud Starter Edition and Cisco Intelligent Automation for Cloud 3.1

There are several differences between Cisco IAC Starter Edition and Cisco Intelligent Automation for Cloud 3.1 that affect the upgrade process:

- In Cisco IAC Starter Edition:
  - 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:
  - A 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 the Shared Zone.

## Supported Upgrade Scenarios

Before performing the upgrade, you must ensure that your current deployment is an upgradeable configuration. The following tables describe the possible deployment scenarios:

- For each deployment scenario, [Table 10-1](#) describes the actions taken by the upgrade process.
- If your setup falls into the scenario described in [Table 10-2](#), you must take the required action. After that action has been completed, your deployment will fall into one of the scenarios described in [Table 10-1](#).

In these tables:

- **Dedicated** means that a resource is assigned and only used by one organization.
- **Shared** means that a resource is used by more than one organization.

**Figure 10-1** Supported Upgrade Scenarios

| Scenario | Organization Resource Pool | Organization Datastore | Organization Network       | Upgrade Behavior                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------|----------------------------|------------------------|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1        | Dedicated                  | Dedicated              | Dedicated                  | No action required. The upgrade process creates a new VDC, and associates the same organization-specific resource pool, datastore, and networks with the organization-specific VDC.<br><br>All virtual and physical servers that belong to this organization are associated with the organization-specific VDC.                                                                                                                                                                                                                                                                      |
| 2        | Dedicated                  | Shared                 | Dedicated                  | Create a new organization VDC, associating the same organization-specific resource pool and networks with the organization-specific VDC. Multiple organization-specific VDCs will share the same datastore.<br><br>All virtual and physical servers that belong to this organization are associated with the organization-specific VDC.                                                                                                                                                                                                                                              |
| 3        | Dedicated                  | Dedicated/<br>Shared   | Dedicated and<br>Community | Create a new organization VDC, associating the same resource pool and datastore with the organization-specific VDC. Dedicated organization networks are associated with the organization VDC.<br><br>All virtual servers that belong to this organization are associated with the organization VDC. Existing virtual servers on community networks are grandfathered in under the organization VDC. However, new virtual servers can only be provisioned on organization-specific networks. No new virtual servers can be provisioned in community networks in the organization VDC. |

Figure 10-1 Supported Upgrade Scenarios

| Scenario | Organization Resource Pool | Organization Datastore | Organization Network | Upgrade Behavior                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------|----------------------------|------------------------|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4        | Dedicated                  | Dedicated/<br>Shared   | Community            | <ol style="list-style-type: none"> <li>1. Create a new organization VDC, associating the same resource pool and datastore with organization-specific VDC. All virtual servers that belong to this organization are associated with the organization VDC. Existing virtual servers on community networks are grandfathered in under the organization VDC.</li> <li>2. After the upgrade is complete, a dedicated organization-specific network must be added to this organization VDC using the "Add Network to VDC" action in the My VDCs portlet. No new virtual servers can be provisioned in community networks in the organization VDC.</li> </ol> |

Table 10-1 Unsupported Upgrade Scenarios

| Scenario | Organization Resource Pool | Organization Datastore | Organization Network     | Required Action                                                                                                                                                                                                                                                                                                                              |
|----------|----------------------------|------------------------|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5        | Shared                     | Dedicated/<br>Shared   | Dedicated /<br>Community | Multiple organizations that share the same resource pool is not supported in Cisco IAC 3.1. Upgrade prerequisites must be met by <a href="#">Verify the Intelligent Automation for Cloud 3.1 Upgrade Prerequisites, page 10-6</a> . After the upgrade prerequisites are met, the upgrade will fall into scenarios listed in the table above. |

## Actions Performed by the Upgrade Process

The upgrade process:

1. Creates a POD (Point of Delivery) containing the infrastructure platform elements defined in Starter Edition.
2. Updates the information for the Cloud Administration Organization to be Cisco IAC 3.1-compliant.
3. Creates a Virtual Data Center for each organization registered in Starter Edition.
4. Converts the flat Starter Edition organization structure to the hierarchical 3.1 organization structure.
5. Creates queues for each organization to support the new Cisco IAC approval functionality.
6. Moves the server associated from the Starter Edition Organization to the organization's VDC.

# Upgrade to Cisco Intelligent Automation for Cloud 3.1

The following table summarizes the steps required to upgrade from Cisco IAC Starter Edition 3.0.2 to Cisco IAC 3.1. These steps provide a high-level overview of the upgrade process; subsequent sections provide additional details.

**Table 10-2** Upgrade Process Summary

|         | Task                                                                                                                                                                      | See                                                                                              |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Step 1  | Back up the Cloud Portal and Tidal Enterprise Orchestrator (TEO) databases.                                                                                               | <a href="#">Back Up the Cloud Portal and TEO Databases, page 10-6</a>                            |
| Step 2  | Deploy the TEO 2.3.4 content update.                                                                                                                                      | <a href="#">Deploy the TEO 2.3.4 Content Update, page 10-6</a>                                   |
| Step 3  | Verify that the upgrade prerequisites have been met on Cisco IAC Starter Edition 3.0.2.                                                                                   | <a href="#">Verify the Intelligent Automation for Cloud 3.1 Upgrade Prerequisites, page 10-6</a> |
| Step 4  | Apply the Cisco Cloud Portal 9.4 Patch. To find the patch version for this release, see the <a href="#">Cisco Intelligent Automation for Cloud Compatibility Matrix</a> . | <a href="#">Apply the Cisco Cloud Portal 9.4 Patch, page 10-8</a>                                |
| Step 5  | Upgrade the Cisco IAC 3.1 REX adapter.                                                                                                                                    | <a href="#">Upgrade the REX Adapter, page 10-8</a>                                               |
| Step 6  | Deploy Cisco IAC 3.1 Upgrade Cloud Portal content.                                                                                                                        | <a href="#">Deploy Cisco IAC CP Upgrade Content, page 10-8</a>                                   |
| Step 7  | Deploy the service catalog packages.                                                                                                                                      | <a href="#">Deploy Service Catalog Packages, page 10-8</a>                                       |
| Step 8  | Deploy the portal packages.                                                                                                                                               | <a href="#">Deploy Portal Packages, page 10-9</a>                                                |
| Step 9  | Set permissions for portals and portlets.                                                                                                                                 | <a href="#">Set Permissions for Portals and Portlets, page 10-9</a>                              |
| Step 10 | Set permissions for the Upgrade Wizard portal page.                                                                                                                       | <a href="#">Set Permission for Upgrade Wizard Portal Page, page 10-9</a>                         |
| Step 11 | Configure the contact information for service queue notifications.                                                                                                        | <a href="#">Configure Contact Information for Service Queue Notifications, page 10-9</a>         |
| Step 12 | Configure the email notification templates.                                                                                                                               | <a href="#">Configure the Email Notification Templates, page 10-10</a>                           |
| Step 13 | Set permissions for the roles groups.                                                                                                                                     | <a href="#">Set Permissions for the Roles Groups, page 10-10</a>                                 |
| Step 14 | Change the Home Organization Unit of the nsAPI user.                                                                                                                      | <a href="#">Change the Home Organization Unit of the nsAPI User, page 10-10</a>                  |
| Step 15 | Configure agent properties.                                                                                                                                               | <a href="#">Configure Agent Properties, page 10-10</a>                                           |
| Step 16 | Run discovery.                                                                                                                                                            | <a href="#">Run Discovery, page 10-11</a>                                                        |
| Step 17 | Register discovered resources.                                                                                                                                            | <a href="#">Register Discovered Resources, page 10-12</a>                                        |
| Step 18 | Run Cisco IAC 3.1 Upgrade Wizard to move data from Cisco IAC Starter Edition 3.0.2 service items to Cisco IAC 3.1 Service Items.                                          | <a href="#">Run the Upgrade Wizard, page 10-12</a>                                               |
| Step 19 | Remove the Starter Edition Portal pages.                                                                                                                                  | <a href="#">Remove the Starter Edition Portal Pages, page 10-14</a>                              |

## Back Up the Cloud Portal and TEO Databases

- Step 1** Create backup files for the following Cloud Portal and TEO databases on your database server:

| Database      | Description                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------------------|
| RequestCenter | Cloud Portal database used for requesting services, orchestrating request fulfillment, and fulfilling services. |
| Datamart      | Cloud Portal analytics and analysis database used for reporting within the solution.                            |
| TEOProcess    | TEO database that displays the properties for the TEO performance database.                                     |
| TEOReporting  | TEO database that generates reports for viewing process execution history and auditing process changes.         |

For information and instructions about backing up databases in SQL Server Management Studio, see [Create a Full Database Backup \(SQL Server\)](#) at msdn.microsoft.com or the documentation that came with the software.

For information and instructions about backing up databases in Oracle Database, see the [Oracle® Database Administrator's Guide 11g Release 2 \(11.2\)](#) at oracle.com or the documentation that came with the software.

- Step 2** Proceed to [Deploy the TEO 2.3.4 Content Update](#).

## Deploy the TEO 2.3.4 Content Update

For instructions, see [Import the Automation Packs in Tidal Enterprise Orchestrator, page 2-2](#). After you have completed this task, return to this chapter and proceed to [Verify the Intelligent Automation for Cloud 3.1 Upgrade Prerequisites](#).

## Verify the Intelligent Automation for Cloud 3.1 Upgrade Prerequisites

- Step 1** Import and deploy the `CP_Upgrade_3-0-2.xml` Cloud Portal catalog deployer package in the Cisco IAC Starter Edition 3.0.2 environment.
- On the TEO server, navigate to the location where the files were extracted during the automation pack import process. By default, the files are copied to the following location on the TEO server:
 


```
C:\Users\\Documents\Cisco\Tidal Enterprise Orchestrator\Extracted Data\IAC 31 Upgrade
```
  - Copy the following files to a folder on the Cloud Portal server:
 

```
CP_Upgrade_3-0-2.xml
```
- Step 2** Navigate to the **My Services** module.
- Step 3** Run the **Check Upgrade Prerequisites** service under the **Upgrade** service group.

- Step 4** If there are organizations sharing the same resource pool, they will be displayed in the table. For example:

| Separate these orgs into their own resource pool. |                                  |
|---------------------------------------------------|----------------------------------|
| Organization Name                                 | Resource Pool Name               |
| IACAdmin                                          | IAC/AUSTIN-LAB/IA-UCS-601-41/DEV |
| IAC Upgrade                                       | IAC/AUSTIN-LAB/IA-UCS-601-41/DEV |
| IAC Migrate                                       | IAC/AUSTIN-LAB/IA-UCS-601-41/DEV |

- Step 5** These organizations must be separated into their own resource pool. To create new resource pools for these organizations:
- In your VMware vCenter Server, create a new resource pool to contain the organization's servers.
  - Move the virtual servers associated with the organization into the new resource pool in VMware Center Server.
  - From the Organization Management portal page, choose **Modify Organization**. Change the VMware vCenter Resource Pool property to the new resource pool. For example:

**Modify Organization**  
 Modify the properties of an existing organization.

---

**Modify Organization Properties**

★ Organization Name:  Select the name of the organization.

Organization Description:

★ **VMware vCenter Resource Pool:**  Modify the full path to the VMware vCenter resource pool that will serve virtual machines deployed by the organization users.

★ **VMware vCenter Datastore Path:**  Modify the full path to the VMware vCenter datastore from which storage will be provided to virtual machines deployed by the organization users.

- Step 6** Proceed to [Apply the Cisco Cloud Portal 9.4 Patch](#).

## Apply the Cisco Cloud Portal 9.4 Patch

**Step 1** Download and extract the hotfix package, which includes a Readme file.



**Note** To find the patch version for this release, see the [Cisco Intelligent Automation for Cloud Compatibility Matrix](#).



**Note** The package name is the same for both Windows and Linux.

**Step 2** Follow the instructions in the Readme for applying the hotfix. The instructions provide important steps for copying extracted files to different deployed directories.

**Step 3** Proceed to [Upgrade the REX Adapter](#).

## Upgrade the REX Adapter

For instructions, see [Chapter 3, “Installing the REX Adapter”](#). After you have completed this task, return to this chapter and proceed to [Deploy Cisco IAC CP Upgrade Content](#).

## Deploy Cisco IAC CP Upgrade Content

**Step 1** On the TEO server, navigate to the location where the files were extracted during the automation pack import process. By default, the files are copied to the following location on the TEO server:

```
C:\Users\\Documents\Cisco\Tidal Enterprise Orchestrator\Extracted Data\IAC 31 Upgrade
```

**Step 2** Copy the following files to a folder on the Cloud Portal server:

- CP\_Upgrade\_Common\_3-1.xml
- CP\_Upgrade\_Services\_3-1.xml

**Step 3** Import and Deploy the CP\_Upgrade\_Common\_3-1.xml and CP\_Upgrade\_3-1.xml files using the procedure in [Import and Deploy Service Catalogs, page 4-4](#).

**Step 4** Proceed to [Deploy Service Catalog Packages](#).

## Deploy Service Catalog Packages

The Cisco IAC service catalog content is included in files that were extracted when the Intelligent Automation for Cloud Starter automation pack was imported to TEO. These files must be imported and deployed in Cloud Portal for the Cisco IAC upgrade.



To deploy service catalog packages:

- 
- Step 1 [Copy Service Catalog Files to Cloud Portal Server, page 4-4.](#)
  - Step 2 [Import and Deploy Service Catalogs, page 4-4.](#)
  - Step 3 After you have deployed the service catalogs, return to this chapter and proceed to [Deploy Portal Packages.](#)
- 

## Deploy Portal Packages

The Cisco IAC portal and portlet content is included in files that were extracted when the Intelligent Automation for Cloud automation pack was imported to TEO. These files must be imported and deployed in Cloud Portal for the Cisco IAC upgrade. After deployment, you must also configure the portals and portlets.

To deploy portal packages, complete the following tasks in [Chapter 4, “Configuring Cisco Cloud Portal and Deploying Cisco Intelligent Automation for Cloud Content”](#):

- 
- Step 1 [Copy the Cisco IAC Portlets Package and Extract Files, page 4-5.](#)
  - Step 2 [Configure Cloud Portal Stylesheets, page 4-6.](#)
  - Step 3 [Import and Deploy Portal Pages, page 4-8](#)
  - Step 4 After you have completed these tasks, return to this chapter and proceed to [Set Permissions for Portals and Portlets.](#)
- 

## Set Permissions for Portals and Portlets

To set the permissions for portals and portlets, follow the instructions in [Set Permissions for Portals and Portlets, page 4-12](#). After you have completed this task, proceed to [Set Permission for Upgrade Wizard Portal Page.](#)

## Set Permission for Upgrade Wizard Portal Page

To set the permissions for the Upgrade Wizard portal page, follow the instructions in [Set Permissions for Portals and Portlets, page 4-12](#). After you have completed this task, proceed to [Configure Contact Information for Service Queue Notifications.](#)

## Configure Contact Information for Service Queue Notifications

You must configure the queue configuration settings with email addresses that will receive email notifications for changes in service queues. You must configure email addresses for each queue.

To assign email addresses for queue notifications, follow the instructions in [Assign Mail Addresses for Queue Notifications, page 6-10](#). After you have completed this task, return to this chapter and proceed to [Configure the Email Notification Templates.](#)

## Configure the Email Notification Templates

Before users can start ordering cloud services, you must configure the email notification templates with the relevant sender and recipient addresses.

To deploy configure the email templates, follow the instructions in [Configure the Email Notification Templates, page 6-12](#). After you have completed this task, proceed to [Set Permissions for the Roles Groups](#).

## Set Permissions for the Roles Groups

Set permissions for the Cisco IAC roles groups:

- 
- Step 1 [Assign Additional Permissions for the Cloud Provider Technical Administrator Role, page 4-17](#).
  - Step 2 [Assign Additional Permissions for the Organization Technical Administrator Role, page 4-22](#).
  - Step 3 [Assign Additional Permissions for the Server Owner Roles, page 4-23](#).
  - Step 4 After you have completed this task, return to this chapter and proceed to [Change the Home Organization Unit of the nsAPI User](#).
- 

## Change the Home Organization Unit of the nsAPI User

Set the home organization unit for the nsAPI user to Cloud Administration.

- 
- Step 1 Choose **Organization Designer** from the module drop-down list and select the **People** tab.
  - Step 2 Enter `nsapi` in the People search box, click **Search**, and select the nsAPI user that is found.
  - Step 3 Select **Org Units** in the right-hand navigation bar.
  - Step 4 Click **Add Organizational Units**.
  - Step 5 Enter `*` in the Search for Organizational Units search bar and click **Search**.
  - Step 6 Select **Cloud Administration** and click **Add**.
  - Step 7 Select the **Cloud Administration OU** and click **Assign as Home**.
  - Step 8 Proceed to [Configure Agent Properties](#).
- 

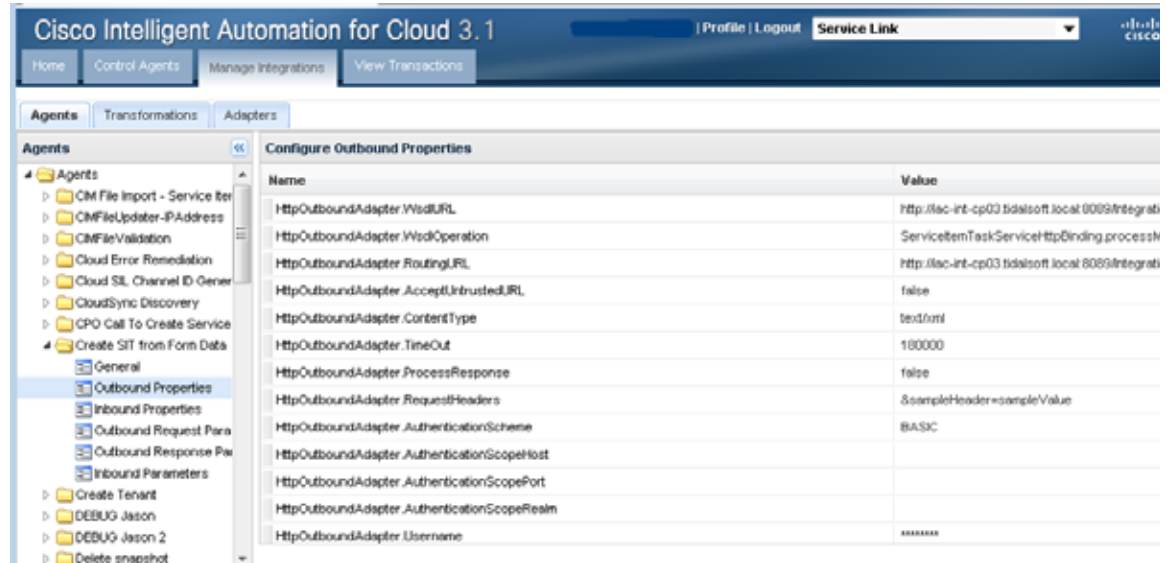
## Configure Agent Properties

To configure agent properties for all REX agents and HTTP agents, complete the following tasks, in the order shown below, to set configure agent properties.

- 
- Step 1 [Set Username and Password for REX Set REX Agent Properties, page 6-6](#).
  - Step 2 [Start the REX Set Agent Properties Agent, page 6-7](#).
  - Step 3 [Set REX Agent Configuration, page 6-7](#).

- Step 4** [Set HTTP Agent Configuration, page 6-9.](#)
- Step 5** Set the username and password for the Create SIT from Form Data agent. The username and password should be set to the nsAPI user name and password.
- Choose **Service Link** from the module drop-down list, then click the **Manage Integrations** tab.
  - In the Agents pane on the left, expand **Create SIT from Form Data** and click **Outbound Properties**.

**Figure 10-2** Create SIT from Form Data



- In the HttpOutboundAdapter.Username field, enter the login name that you created in the Create Person form for the nsAPI user.
  - In the HttpOutboundAdapter.Password field, enter the password in the Create Person form for the nsAPI user.
  - Click **Save**.
- Step 6** Using the procedure in [Set Username and Password for REX Set REX Agent Properties, page 6-6](#), set the username and password for the **REX Upgrade 30x OU agent** to the REX user name and password.
- Step 7** [Start All Other Agents, page 6-10.](#)
- Step 8** After you have completed these tasks, proceed to [Run Discovery](#).

## Run Discovery

- Step 1** See the *Cisco Intelligent Automation for Cloud 3.1 User Guide*, chapter 2, [Managing Cloud Infrastructure Discovery](#).
- Step 2** Proceed to [Register Discovered Resources](#).

## Register Discovered Resources

After discovery runs, discovered resources such as VMware vCenter VM Templates and Datastores, Cisco Server Provisioner Operating System Templates, and UCS Manager Service Profiles must be registered before they can be used.

- 
- Step 1** Register the following VMware vCenter resources:
- Datastores (see [Register a Datastore, page 7-12](#))
  - Virtual Machine template (see [Registering a Virtual Machine Template, page 8-1](#))
- Step 2** Register the Server Provisioner Operating System Templates (see [Registering an Operating System Template, page 8-2](#)):
- Step 3** Register UCS Manager service profile templates (see [Registering a UCS Service Profile Template, page 8-3](#)).




---

**Note** This is required only for physical server provisioning.

---

- Step 4** Proceed to [Run the Upgrade Wizard](#).
- 

## Run the Upgrade Wizard

Migrate data from Cisco IAC Starter Edition 3.0.2 to Cisco IAC 3.1.

- 
- Step 1** Choose **My Workspace** from the module drop-down list, then click the **Upgrade Wizard** tab to open the Cisco IAC 3.1 Upgrade Wizard.
- Step 2** Click **Upgrade Cloud Admin Organization and POD**. On the form, enter the following:
- a. Enter the Company Abbreviation, which should be a four-letter abbreviation for the company.
  - b. Enter the POD name and Description. A POD will be created using the existing platform elements defined in Cisco IAC.
  - c. Select the UCS VLAN and vCenter Portgroup that is used for the Cisco Server Provisioner.
  - d. Click **Submit Order**.
- Step 3** Click **Set Provisioning Settings**. To set provisioning settings, follow the instructions in [Set Provisioning Settings, page 7-6](#).
- Step 4** Click **Upgrade Virtual Data Centers**. On the form, perform the following:
- a. Organization VDCs table - modify the Maximum Number of Virtual Servers, Maximum Number of vCPUs, Maximum Number of Snapshots, Maximum Total Storage (GB), and Maximum Number of Physical Servers in the table, if needed.
  - b. The Organization Networks table shows the network names associated with the organization's VDC. This is a read-only table for informational purposes only.
  - c. The Organization VDC ownership shows the VDC name being created and the organization that owns that VDC. This is a read-only table for informational purposes only.
  - d. Click **Submit Order**.

- Step 5** Click **Upgrade Organization Structure** .
- The Organization List shows the list of organizations to be updated to a hierarchical organization unit structure. This field is read-only is for informational purposes only.
  - Parent Organization shows the organization which is the parent of the other organizations. This field is read-only is for informational purposes only.
  - Click **Submit Order**.
- Step 6** Click **Create Shared Zone**. This creates a new shared zone for Cisco IAC 3.1. Any previously used Community Networks will be associated with the Cisco IAC 3.1 Shared Zone. For more information about creating a shared zone, see [Set Up a Shared Zone, page 7-13](#).
- Step 7** Click **Assign Servers to Virtual Data Centers**. This assigns all Virtual and Physical Servers owned by an organization to the organization's Virtual Data Center. Perform the following manual steps to do this:
- Copy the `ciac.jar` located on the TEO server under:
 

```
C:\Users\\Documents\Cisco\Tidal Enterprise Orchestrator\Extracted Data\IAC
31 Upgrade
```

 into the `<JBOSS_DIR>/standalone/deployments/RequestCenter.war/WEB-INF/lib` folder on the Cloud Portal server.
  - Open a Windows or UNIX command shell.
  - Change directory to `<JBOSS_DIR>/standalone/deployments/RequestCenter.war/WEB-INF/lib`.
  - Run `java -jar ciac.jar`.
  - Enter the following information:
    - **Database Type:** Enter `SQLSERVER` or `ORACLE` for the Database Type
    - **Database Hostname:** Enter the fully qualified hostname of the database server
    - **Database Port:** Enter the port number of the database. Default port number for SQL Server is 1433. Default port number for Oracle is 1521.
    - **Database Name** (for `SQLServer`): Enter the database name. Default database name is `RequestCenter`.
    - **Oracle SID** (for `Oracle`): Enter the Oracle SID. Default Oracle SID is `ORCL`.
    - **Username:** Enter the Request Center database username. This is case-sensitive.
    - **Password:** Enter the password for the Request Center database user. This is case-sensitive.

**Figure 10-3** Example Run:

```
C:\jboss-as-7.1.1.Final\standalone\deployments\RequestCenter.war\WEB-INF\lib>java -jar
ciac.jar
Please enter the database connection information.
Database Type [SQLSERVER]:
Database Hostname [localhost]: IAC-BVT-US05.tidalsoft.local
Database Port [1433]:
Database Name [RequestCenter]:
Username [RCUSER]: RCUser
Password:
Testing database connection: Success!
Getting repository instance...
Updating Virtual Server...
Processing Complete.
Plugin Execution completed successfully.
```

- f. After the utility executes successfully, delete the `ciac.jar` from `<JBOSS_DIR>/standalone/deployments/RequestCenter.war/WEB-INF/lib`.
- 

## Remove the Starter Edition Portal Pages

Remove the old Starter Edition portal pages.

---

- Step 1 Choose Portal Designer from the module drop-down list.
  - Step 2 Select the Portal Pages tab.
  - Step 3 Expand the Cisco IAC Starter Edition Folder.
  - Step 4 Select the Configuration Wizard portal page.
  - Step 5 Click **Delete**.
  - Step 6 Repeat steps 3-5 for the remaining portal pages:
    - Network Management
    - Organization Management
    - System Resources
    - System Setup
    - User Management
  - Step 7 Select the Cisco IAC Starter Edition Folder.
  - Step 8 Click **Delete**.
  - Step 9 Expand the My Workspace Folder.
  - Step 10 Select the My Servers portal page.
  - Step 11 Click **Delete**.
  - Step 12 Repeat steps 9-11 for the Order Servers portal page.
- 

The upgrade is now complete. To make changes to your current Cisco IAC 3.1 configuration, see the following chapters:

- [Chapter 8, “Post-Configuration Options”](#)
- [Set System-wide Service Options, page 7-7](#)



## APPENDIX **A**

# Setting Up Directory Integration

---



Note

**This appendix provides examples of setting up directory integration in Microsoft Active Directory.** There are many scenarios for directory integration configuration based on the directory product and settings, so it is likely that your environment will vary from what is presented here. However, the required sequence of configuring directory integration would be the same.

For instructions on configuring directory integration if your setup varies, *see* the [Cisco Service Portal 9.4 Integration Guide](#). It is strongly recommended that you review this appendix before proceeding with directory integration configuration, and refer to it as you work through the necessary steps.

---

Cisco Cloud Portal can integrate with directory servers to synchronize user information. This synchronization can be initiated whenever a user logs on or is selected or during Person Lookup in Cloud Portal.

Prior to configuring integration in Cloud Portal, you must have a directory server installed and populated with corporate data.

This appendix includes the following sections:

- [Prerequisites, page A-2](#)
- [Introduction, page A-2](#)
- [Step 1: Configuring the LDAP Server, page A-3](#)
- [Step 2: Configure Authentication, page A-5](#)
- [Step 3: Configure Authorization \(Optional\), page A-8](#)
- [Step 4: Enable Directory Integration, page A-9](#)



Note

**When you have completed directory integration, return to [Import and Deploy Intelligent Automation for Cloud Service Catalogs, page 4-3](#) in [Chapter 4, “Configuring Cisco Cloud Portal and Deploying Cisco Intelligent Automation for Cloud Content,”](#) to pick up where you left off in the Cisco IAC configuration process.**

---

# Prerequisites

Before configuring directory integration for use with Cisco IAC, you must complete the following tasks:

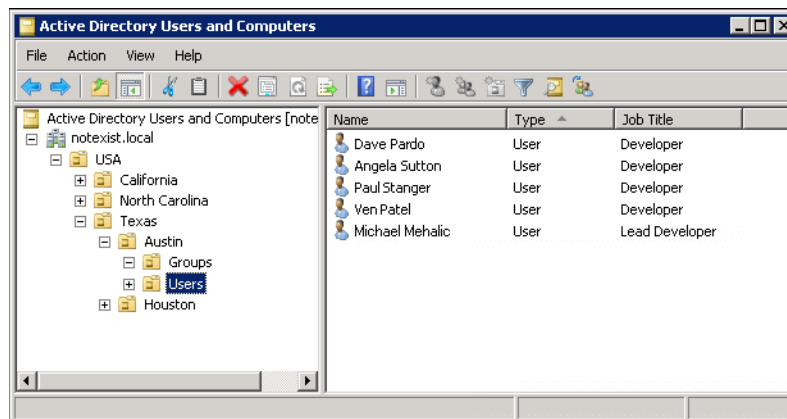
- Set up organizational unit structure on the LDAP server. [Figure A-1](#) provides an example, but you can set up the structure in any way.



**Note** If you do not have privileges to perform this task on the LDAP server, seek help from your LDAP server administrator.

- Create the following user accounts in the Users folder on the LDAP server:
  - nsAPI user
  - A user account (any username) with “Read MemberOf” permissions that will be used for performing authentication, directory searches, and user imports into the cloud portal.

**Figure A-1** Example User Accounts in Active Directory



# Introduction

Although directory scenarios vary depending on the directory product and settings, there is a **required** sequence for configuring directory integration for use with Cisco IAC:

- [Step 1: Configuring the LDAP Server, page A-3](#)
- [Step 2: Configure Authentication, page A-5](#)
  - [Configure Mappings, page A-5](#)
  - [Configure Events, page A-6](#)
- [Step 3: Configure Authorization \(Optional\), page A-8](#)
  - [Create a Security Group for Each User Role on the LDAP Server, page A-8](#)
  - [Add the nsAPI User to the Cloud Administration Group, page A-9](#)
  - [Configure User Role Mappings, page A-9](#)
- [Step 4: Enable Directory Integration, page A-9](#)



# Step 1: Configuring the LDAP Server

The first step is to add a datasource and test the connection in Cloud Portal. The instructions in this section are how one would connect to the LDAP server in the example scenario.

- Step 1** In Cloud Portal, choose **My Workspace** from the module drop-down list, then click the **System Setup** tab.
- Step 2** On the System Setup portal, click the **Connections** tab to open the portlet, then click **Directory Server Connection Information**.
- Step 3** Click **Add** to display the Datasources Configuration pane.

**Figure A-2** Directory Integration—Datasources



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

- Step 4** In the Add or Edit a Datasource pane, enter the following information:

| Field                  | Action                                                                    |
|------------------------|---------------------------------------------------------------------------|
| Datasource Name        | Enter a name for the datasource. Do not use spaces or special characters. |
| Datasource Description | <i>Optional.</i> Enter a description of the datasource.                   |

- Step 5** Expand **Select protocol and server product**, then choose the following settings:

| Setting        | Action                                                                                                                                          |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Protocol       | The protocol is always <b>LDAP</b> .                                                                                                            |
| Server Product | Choose <b>Active Directory</b> .<br><b>Note</b> The other server product selections are <b>Sun One</b> and <b>IBM Tivoli Directory Server</b> . |

**Step 6** Expand **Connection Information**, then specify the following required datasource information in the definition area. This information includes lookup user that you set up as a prerequisite.

| Field                 | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authentication Method | Choose <b>Simple</b> (text username and password) from the drop-down list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Mechanism             | Choose <b>Non SSL</b> from the drop-down list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| BindDN                | <p>Enter the bind-distinguished name (BindDN) value for the lookup user. The BindDN looks like the following example:</p> <p style="text-align: center;">CN=Mehalic Michael,OU=Users,OU=Austin,OU=Texas,OU=USA,DC=notexist,DC=local</p> <p>To query the BindDN value, open a command prompt on the Windows server and execute the following command:</p> <p style="text-align: center;"><b>dsquery user -name "[name]*"</b></p>                                                                                                                                                           |
| Host                  | Enter the fully qualified hostname or IP address of the LDAP directory server. For example: dc.notexist.local                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| User BaseDN           | <p>Enter the parent folder under which all users will gain access.</p> <p>For example, if the User BaseDN is OU=Austin,OU=Texas,OU=USA,DC=notexist,DC=local, then all users in the Austin organization will have access.</p>                                                                                                                                                                                                                                                                                                                                                              |
| Port Number           | <p>Enter the port number for the LDAP according to either of the following conditions:</p> <ul style="list-style-type: none"> <li>• For a non-SSL connection, the default port number for LDAP is <b>389</b>.</li> <li>• For an SSL connection, the default port number is for LDAP is <b>636</b>.</li> </ul> <p>You can verify the port number for your LDAP server using either of the following methods:</p> <ul style="list-style-type: none"> <li>• Run the command <b>netstat -an</b> on the domain controller,</li> <li>• Use the SysInternals tool <b>TCPView.exe</b>.</li> </ul> |
| Password              | Enter the password for the user specified as the BindDN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

**Step 7** Click **Update**.

**Step 8** Check the check box next to the newly added datasource and click **Test Connection**. The Test Status column displays OK if the connection is successful.

**Step 9** Keep the form open and proceed to [Step 2: Configure Authentication](#).

## Step 2: Configure Authentication

The second step, configuring authentication, requires two tasks:

- [Configure Mappings, page A-5](#)
- [Configure Events, page A-6](#)

The instructions in this section are how one would complete each task in the example scenario.

### Configure Mappings

The first task in configuring authentication is to assign mapping attributes to user data, including first and last name, login ID, and home organization unit.



**Note**

Active Directory has pre-defined mapping attributes, which are used in this example. However, there are data fields that have no specific Active Directory mapping attributes. In such cases (indicated below), you can assign any mapping attribute that you want to the data field.

- Step 1** In the **Administration** module, click the **Directories** tab.
- Step 2** On the Directory Integration page, click **Mappings** in the menu on the right.
- Step 3** In the Mappings pane, click **Add** to display the Mapping Configuration pane.



**Note**

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

- Step 4** In the “Add or edit a mapping name” pane, specify the following information:

| Field               | Action                                                                 |
|---------------------|------------------------------------------------------------------------|
| Mapping Name        | Enter a name for the mapping. Do not use spaces or special characters. |
| Mapping Description | <i>Optional.</i> Enter a description of the mapping.                   |

- Step 5** In the “Configure mapping attributes” area, enter the required information in the text fields. The following table provides examples of datasource mappings for person data.



**Note**

Active Directory mapping attributes are pre-defined and case-sensitive.



**Note**

For information on how to form expressions, see the documentation that shipped with your directory software.

| Person Data | Mapping Attribute |
|-------------|-------------------|
| First Name  | givenName         |
| Last Name   | sn                |

| Person Data             | Mapping Attribute                                                                                                                                                                                                                                                                                            |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Login ID                | sAMAccountName                                                                                                                                                                                                                                                                                               |
| Personal Identification | sAMAccountName<br><b>Note</b> For this data field, there is no corresponding mapping attribute in Active Directory. In this case, you can assign any mapping attribute you want.                                                                                                                             |
| Email Address           | expr:#email#=(.+)?(#email#):NotExist                                                                                                                                                                                                                                                                         |
| Home Organization Unit  | expr:#department#=(.+)?(#department#):NotExist                                                                                                                                                                                                                                                               |
| Password                | sAMAccountName<br><b>Note</b> There is no mapping attribute for passwords in Active Directory. Instead, you can map it to another attribute (in this example, sAMAccountName). You can also map your own expression. For information, see the documentation that shipped with the Active Directory software. |

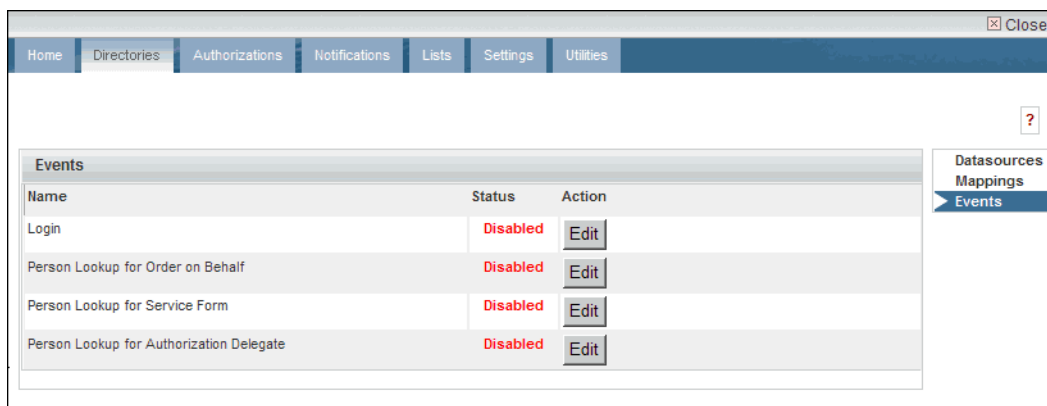
**Step 6** Click **Update**.

**Step 7** Test the mappings using the Data Test Mapping feature. For instructions on enabling then using the Data Test Mapping feature, *see* “Testing Mappings” in Chapter 1, “Directory Integration and API,” in the *Cisco Service Portal 9.4 Integration Guide*.

## Configure Events

**Step 1** Click **Events** in the menu on the right.

**Figure A-3** Directory Integration—Events



**Step 2** In the Events pane, click **Edit** next to the Login event to display the Event Configuration pane.

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

- Step 4** In the Event Configuration pane, click **Add step**, then specify the following information in the Event Step area:

| Field              | Action                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operation          | Choose <b>External Authentication</b> .                                                                                                                                                                                                                                                                                                                                                                                  |
| Additional Options | <p>Click <b>Options</b>, then enter the EUABindDN using the following convention:</p> <p style="text-align: center;">&lt;netbios domain&gt;\#LoginId#</p> <p><b>Note</b> You <b>must</b> provide the EUABindDN value, which is critical for login events. This value is case-sensitive.</p> <p><b>Note</b> This attribute is a pre-defined Active Directory value. The attribute is different for other directories.</p> |

- Step 5** Click **Update** to add the information as the first step in the event.

- Step 6** Click **Add step**.

- Step 7** In the Step 2 row, choose **Import Person** from the Operation drop-down list.

- Step 8** From the Mapping drop-down list, choose the mapping name you specified when you defined mappings (see [Step 2: Configure Authentication, page A-5](#)).

- Step 9** From the Datasource drop-down list, choose the datasource name that you specified in [Step 4 of Step 1: Configuring the LDAP Server, page A-3](#).

- Step 10** Click **Options**, then specify the following information in the Event Step area:

| Field                  | Action                                                                                                                                                                                                                                                                                                   |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Refresh Person Profile | Ensure that the check box is <i>checked</i> .                                                                                                                                                                                                                                                            |
| Refresh Period (Hours) | Leave this field blank. If a value populates the field, delete the value.                                                                                                                                                                                                                                |
| Do not create Group/OU | <ul style="list-style-type: none"> <li>• <b>Organizational Unit</b>—<i>Check</i> the check box. Checking this option prevents a user from logging in to the Cloud Portal Server unless the user's home organization has been onboarded.</li> <li>• <b>Group</b>—<i>Uncheck</i> the check box.</li> </ul> |

- Step 11** Click **Update** to add the information as Step 2.

- Step 12** Click **Update**.

- Step 13** Proceed to one of the following sections:

- If you intend to configure authorization (optional), proceed to [Step 3: Configure Authorization \(Optional\), page A-8](#).
- If you do not intend to configure authorization, skip to [Step 4: Enable Directory Integration, page A-9](#) to complete directory integration setup.

## Step 3: Configure Authorization (Optional)

To configure authorization, you must complete the following steps:

- [Create a Security Group for Each User Role on the LDAP Server, page A-8](#)
- [Add the nsAPI User to the Cloud Administration Group, page A-9](#)
- [Configure User Role Mappings, page A-9](#)

### Create a Security Group for Each User Role on the LDAP Server

In your directory, create one security group for each user role. The name of each group must match exactly the name of the user role:

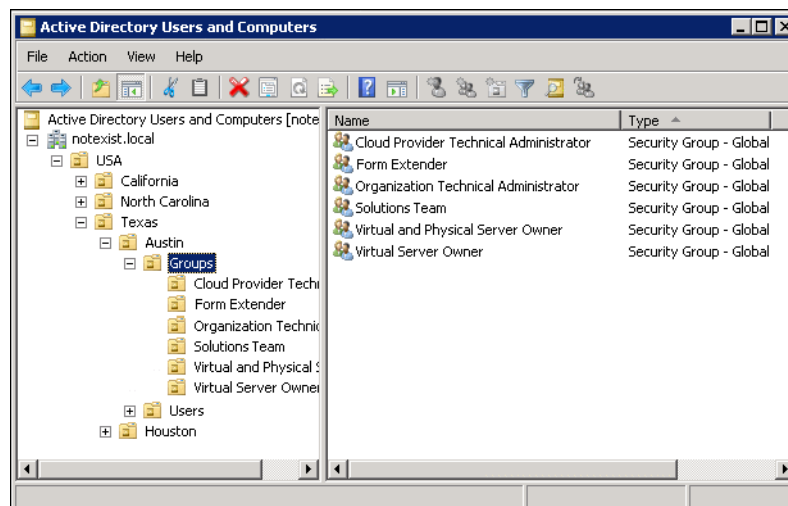
- Cloud Provider Technical Administrator
- Organization Technical Administrator
- Virtual and Physical Server Owner
- Virtual Server Owner
- Solutions Team
- Form Extender

[Figure A-4 on page A-8](#) shows the six security groups in Active Directory.

For instructions on creating security groups on your directory server, see the documentation that came with your directory server software.

After you have completed this task, proceed to [Add the nsAPI User to the Cloud Administration Group](#).

**Figure A-4** Cloud Portal Role Security Groups in an Example LDAP Server Directory Structure



## Add the nsAPI User to the Cloud Administration Group

The nsAPI user account that you created on the LDAP server is used to connect Cloud Portal to TEO. For the nsAPI user account to function properly, you must add it to the Cloud Provider Technical Administrator user group that you created in the directory.

For instructions on adding a user to a user role group on your directory server, see the documentation that came with your directory server software.

When you have completed this task, proceed to the next section, [Configure User Role Mappings](#).

## Configure User Role Mappings

To map the user roles, you specify the location in the directory that contains the six security groups you created for each role.

- 
- Step 1** In Cloud Portal, choose **Administration** from the module drop-down list and click the **Directories** tab.
  - Step 2** On the Directory Integration page, click **Mappings** in the menu on the right.
  - Step 3** In the Mappings pane, click **Edit** beside the mapping name you created when you configured mappings (see [Configure Mappings, page A-5](#)).
  - Step 4** Expand **Optional Person Data Mappings** at the bottom of the page.
  - Step 5** In the Role List field at the bottom of the optional mappings list, enter mapping attributes for role list that assigns the user to one of the six Cloud Portal user groups that you created in the directory. using the convention used for the example scenario (variables for the example appear in boldface):  

```
expr:#memberOf#=(CN=(.*),OU=Groups,OU=Austin,OU=Texas,OU=USA,DC=notexist,DC=local)?($1):
```
  - Step 6** Test the mappings using the Data Test Mapping feature. For instructions on enabling and using the Data Test Mapping feature, see “Testing Mappings” in Chapter 1, “Directory Integration and API,” in the [Cisco Service Portal 9.4 Integration Guide](#).
  - Step 7** Proceed to [Step 4: Enable Directory Integration](#) to complete directory integration setup.
- 

## Step 4: Enable Directory Integration



### Caution

Before you enable directory integration, you must have all user groups configured for use with Cisco IAC. If you do not have all user groups configured before you enable directory integration, you will not be able to log back in to Cloud Portal.

---

- 
- Step 1** Choose **Administration** from the module drop-down list, then click **Personalize Your Site**.
  - Step 2** On the **Customizations** page, scroll down to the Common Settings area and turn the Enable Directory Integration setting **On**.
  - Step 3** Click the **Update** button at the *bottom* of the page.
-

After completing directory integration, return to [Import and Deploy Intelligent Automation for Cloud Service Catalogs, page 4-3](#) in Chapter 4, “Configuring Cisco Cloud Portal and Deploying Cisco Intelligent Automation for Cloud Content,” to resume the Cisco IAC configuration process.





# APPENDIX B

## Solution Prerequisites Checklists

---

Chapter 1, “Solution Prerequisites,” specifies all of the requirements that you must meet before installing Cisco Intelligent Automation for Cloud.

Use the following checklists to ensure that all of the prerequisites are met before the installation:

- [Minimum Hardware Requirements for Platform Elements, page B-2](#)
- [Minimum Software Requirements, page B-3](#)
- [Default Ports and Protocols, page B-4](#)
- [Limitations and Scalability, page B-5](#)
- [Cisco IAC Software Installation Preparation, page B-5](#)
- [Network Requirements, page B-6](#)
- [Storage Management Requirements, page B-6](#)
- [Cisco UCS Manager and Bare Metal Operating System Provisioning Requirements, page B-7](#)
- [VMware Software Requirements, page B-8](#)
- [Directory and Mail Server Requirements, page B-8](#)
- [Organizations and Users Preparation, page B-9](#)
- [Create a Virtual Datacenter, page B-9](#)
- [Create Shared Zones, page B-9](#)
- [Order VM From Template, page B-9](#)
- [Order a VM and Install an Operating System, page B-10](#)
- [Order a Physical Server, page B-10](#)
- [Provision ESXi, page B-10](#)

# Minimum Hardware Requirements for Platform Elements

For more information about these requirements, see [Minimum Hardware Requirements for Platform Elements, page 1-2](#).

**Table B-1** Minimum Hardware Requirements for Platform Elements

| Platform Element                                        | Component  | Server                                                                                                                 | ✓ |
|---------------------------------------------------------|------------|------------------------------------------------------------------------------------------------------------------------|---|
| Tidal Enterprise Orchestrator (TEO) Server <sup>1</sup> | CPU        | 64-bit 2.8 GHz or higher core                                                                                          |   |
|                                                         | Memory     | 2 GB minimum (8 GB or higher recommended)<br>8 GB of RAM (if Microsoft SQL Server is installed on same machine as TEO) |   |
|                                                         | Disk Space | 1 GB of available hard disk space dedicated to TEO                                                                     |   |
| Cisco Cloud Portal                                      | CPU        | Intel Core 2 Dual processor or equivalent                                                                              |   |
|                                                         | Memory     | 4 GB RAM                                                                                                               |   |
|                                                         | Disk Space | 40 GB free hard disk space                                                                                             |   |
| Cisco Cloud Portal Database                             | CPU        | Intel Core 2 Dual processor or equivalent                                                                              |   |
|                                                         | Memory     | 4 GB RAM                                                                                                               |   |
|                                                         | Disk Space | 50 GB free hard disk space                                                                                             |   |
| Cisco Server Provisioner                                | CPU        | EM64T, Intel 64 or AMD64                                                                                               |   |
|                                                         | Memory     | 512 MB                                                                                                                 |   |
|                                                         | Disk Space | 40 GB                                                                                                                  |   |

1. For complete installation prerequisites, see the *Tidal Enterprise Orchestrator Installation and Administration Guide 2.3* on [Cisco.com](https://www.cisco.com).

# Minimum Software Requirements

For more information about these requirements, see [Minimum Software Requirements, page 1-3](#).

**Table B-2** Minimum Software Requirements

| Component                           | Server                   | Requirements                                               | ✓ |
|-------------------------------------|--------------------------|------------------------------------------------------------|---|
| Application Server Operating System | TEO                      | Microsoft Windows Server <sup>1</sup>                      |   |
|                                     | Cloud Portal             | Microsoft Windows Server <sup>1</sup>                      |   |
|                                     |                          | Red Hat Enterprise Linux <sup>1</sup>                      |   |
|                                     | Cisco Server Provisioner | Red Hat or CentOS <sup>1</sup>                             |   |
| Application Server Framework        | TEO                      | .NET Framework <sup>1</sup>                                |   |
|                                     |                          | VMware vSphere PowerCLI <sup>1</sup>                       |   |
|                                     | Cloud Portal             | JBoss® <sup>1</sup>                                        |   |
| Application Software                | TEO                      | TEO <sup>1</sup>                                           |   |
|                                     | Cloud Portal             | Cloud Portal <sup>1</sup>                                  |   |
|                                     |                          | REX adapter                                                |   |
|                                     |                          | Cloud Portal patch <sup>1</sup>                            |   |
| LDAP Server (if using a directory)  | TEO                      | Microsoft Active Directory <sup>1</sup>                    |   |
|                                     | Cloud Portal             | Microsoft Active Directory <sup>1</sup>                    |   |
|                                     |                          | IBM Tivoli™ Directory Server <sup>1</sup>                  |   |
|                                     |                          | Sun Java™ System Directory Server <sup>1</sup>             |   |
| Web Server                          | TEO                      | Microsoft Internet Information Services (IIS) <sup>1</sup> |   |
|                                     | Cloud Portal             | Microsoft Internet Information Services (IIS) <sup>1</sup> |   |
| Database                            | TEO                      | Microsoft SQL Server <sup>1</sup>                          |   |
|                                     |                          | Oracle® Database Enterprise Edition <sup>1</sup>           |   |
|                                     | Portal                   | Microsoft SQL Server <sup>1</sup>                          |   |
|                                     |                          | Oracle Database Enterprise Edition <sup>1</sup>            |   |
| Web Browser                         | TEO                      | Microsoft Internet Explorer® <sup>1</sup>                  |   |
|                                     |                          | Mozilla Firefox <sup>1</sup>                               |   |
|                                     | Portal                   | Microsoft Internet Explorer <sup>1</sup>                   |   |
|                                     |                          | Mozilla Firefox <sup>1</sup>                               |   |
| Virtualization <sup>2</sup>         | Hypervisor               | VMware ESXi <sup>1</sup>                                   |   |
|                                     | Hypervisor Manager       | VMware vCenter/vSphere <sup>1</sup>                        |   |
| Physical Server Provisioning        | Cisco UCS Manager        | Cisco UCS blades <sup>1</sup>                              |   |

1. See the [Cisco Intelligent Automation for Cloud Product Compatibility Matrix](#) for the supported version or versions.

2. **For Cisco IAC, vCenter object names cannot contain forward slashes.** For more information, please see the Caution in [VMware Software Preparation, page 1-9](#).

# Default Ports and Protocols

For more information about these requirements, see [Default Ports and Protocols, page 1-4](#).

**Table B-3** Requirements—Default Ports and Protocols

| Application              | Default Port | Protocol | Description                                                                                                                        | ✓ |
|--------------------------|--------------|----------|------------------------------------------------------------------------------------------------------------------------------------|---|
| Cisco Cloud Portal       | 8080         | TCP      | Client web browser connections to the Cloud Portal RequestCenter; TEO communications to the Cisco Cloud Portal inbound web service |   |
| TEO                      | 2081         | TCP      | User Web browser connections to the TEO web console                                                                                |   |
|                          | 61525        | TCP      | TEO Console access to the TEO Server                                                                                               |   |
|                          | 61526        | TCP      | Web Service (API) communication using HTTPS protocol from the Cisco Cloud Portal to the TEO web service                            |   |
|                          | 61527        | TCP      | Web Service (API) communication using HTTP protocol from the Cisco Cloud Portal to the TEO web service                             |   |
| Cisco Server Provisioner | 80           | TCP      | HTTP web service communication between TEO and Cisco Server Provisioner                                                            |   |
|                          | 21           | TCP      | FTP protocol used for Cisco Server Provisioner client provisioning                                                                 |   |
|                          | 67           | UDP      | BOOTP protocol used for Cisco Server Provisioner client provisioning                                                               |   |
|                          | 111          | UDP      | TFTP protocol used for Cisco Server Provisioner client provisioning                                                                |   |
|                          | 139          | TCP/UDP  | NetBios protocol used for Cisco Server Provisioner client provisioning                                                             |   |
|                          | 445          | TCP/UDP  | SMB protocol used for Cisco Server Provisioner client provisioning                                                                 |   |
|                          | 4011         | TCP      | BINL protocol used for Cisco Server Provisioner client provisioning                                                                |   |

# Limitations and Scalability

For more information about these requirements, see [Limitations and Scalability, page 1-5](#).

**Table B-4** Requirements—Limitations and Scalability

| Entity                          | Limitations                                                                | ✓ |
|---------------------------------|----------------------------------------------------------------------------|---|
| Cisco UCS Manager               | 1 instance per delivery (POD). Each POD can contain up to 160 blades/host. |   |
| TEO server                      | 1 server                                                                   |   |
| Cisco Server Provisioner server | 1 or more. Each CSP can be associated to one or more PODs.                 |   |
| Registered users                | Up to 1,000; up to 200 concurrent users                                    |   |
| Service items (concurrent)      | Up to 10,000                                                               |   |
| VMware vCenter <sup>1</sup>     | 1 instance                                                                 |   |

1. For Cisco IAC, vCenter object names cannot contain forward slashes. For more information, please see the Caution in [VMware Software Preparation, page 1-9](#).

## Cisco IAC Software Installation Preparation

For more information about these requirements, see [Intelligent Automation for Cloud Software Installation Preparation, page 1-6](#).

**Table B-5** Requirements—Installing an Operating System on the Application Server

| Components                                                | ✓ |
|-----------------------------------------------------------|---|
| Operating system is installed on TEO                      |   |
| Operating system is installed on Cisco Cloud Portal       |   |
| Operating system is installed on Cisco Server Provisioner |   |

**Table B-6** Requirements—Installing Database Servers

| Components                                         | ✓ |
|----------------------------------------------------|---|
| Database server is available to TEO                |   |
| Database server is available to Cisco Cloud Portal |   |

**Table B-7** Requirements—Installing Cisco IAC on Application Server

| Components                                                                                       | ✓ |
|--------------------------------------------------------------------------------------------------|---|
| Application Server (JBoss, WebLogic, or WebSphere) is installed on the Cisco Cloud Portal server |   |

# Network Requirements

For more information about these requirements, see [Networks, page 1-7](#).

**Table B-8 Requirements—Networks**

| Requirement                                                                                                                                                                                                                                                                                                                                               | ✓ |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| At least one VLAN to use as a destination network for provisioning servers                                                                                                                                                                                                                                                                                |   |
| A VLAN for Cisco Server Provisioner to use as its private PXE VLAN, set up in UCS Manager and in vCenter <sup>1,2</sup><br><br>This is only required if any of the following features are enabled: Virtual Machine and Install OS Ordering, Physical Server Ordering, or ESXi Provisioning in <a href="#">Set System-wide Service Options, page 7-7</a> . |   |
| A VLAN for use as an infrastructure network. This is only required if ESXi Provisioning is enabled in <a href="#">Set System-wide Service Options, page 7-7</a> .                                                                                                                                                                                         |   |

1. For more information about Cisco Server Provisioner, see the [LinMin Bare Metal Provisioning User's Guide](#) on LinMin.com.
2. **For Cisco IAC, vCenter object names cannot contain forward slashes.** For more information, please see the Caution in [VMware Software Preparation, page 1-9](#).

# Storage Management Requirements

For more information about these requirements, see [Storage Management Preparation, page 1-7](#).

**Table B-9 Requirements—Storage Management**

| Requirement                                | ✓ |
|--------------------------------------------|---|
| Create storage and configure as datastores |   |

# Cisco UCS Manager and Bare Metal Operating System Provisioning Requirements

For more information about these requirements, see [Cisco UCS and Bare Metal Operating System Provisioning Preparation, page 1-7](#).

- UCS Manager Installation and Configuration—[Table B-10](#)
- Creating UCS Manager Pools and Policies—[Table B-11](#)
- Creating Cisco UCS Manager Service Profile Templates—[Table B-12](#)

**Table B-10 Requirement—Installing and Configuring UCS Manager**

| Requirement                                                         |   |
|---------------------------------------------------------------------|---|
| UCS Manager is installed and configured before installing Cisco IAC | ✓ |

**Table B-11 Requirements—Creating UCS Manager Pools**

| Requirement      |   |
|------------------|---|
| UUID suffix pool | ✓ |
| MAC address pool |   |
| WWNN pool        |   |
| WWPN pool        |   |



Note

The following requirements apply if either the Physical Server Ordering or ESXi Provisioning options are enabled in [Set System-wide Service Options, page 7-7](#).

**Table B-12 Requirements—Creating Cisco UCS Manager Service Profile Templates and Policies**

| Requirement                                                                                                                                                                                                                                          |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| A hypervisor service profile template, per cluster, with the same quantity and configuration of vNICs as on other hosts in the same cluster. The native VLAN for the first vNIC should be set to the Management VLAN for that vCenter <sup>1</sup> . | ✓ |
| <b>Note</b> Required only if ESXi Provisioning is enabled in <a href="#">Set System-wide Service Options, page 7-7</a> .                                                                                                                             |   |
| At least one service profile template for physical server provisioning.                                                                                                                                                                              |   |
| <b>Note</b> Required only if Physical Server Ordering is enabled in <a href="#">Set System-wide Service Options, page 7-7</a> .                                                                                                                      |   |
| A local boot policy assigned to the physical server service profile template which is set to boot from local disk                                                                                                                                    |   |
| A boot policy named "PXEBoot" which is configured to boot from the network                                                                                                                                                                           |   |
| <b>Note</b> This name is mandatory                                                                                                                                                                                                                   |   |

**Table B-12** Requirements—Creating Cisco UCS Manager Service Profile Templates and Policies

| Requirement                                                                                                                                                                            |   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| Provisioning templates are prepared according to Cisco Server Provisioner product documentation ( <i>see the <a href="#">Cisco Server Provisioner User's Guide</a> on LinMin.com</i> ) | ✓ |
| UCS blades for provisioning VMware ESXi hypervisor hosts have at least one local drive                                                                                                 |   |

1. For Cisco IAC, vCenter object names cannot contain forward slashes. For more information, please see the Caution in [VMware Software Preparation, page 1-9](#).

## VMware Software Requirements



### Caution

For Cisco IAC, vCenter object names cannot contain forward slashes. For more information, please see [VMware Software Preparation, page 1-9](#).

**Table B-13** Requirements—VMware Software Installation

| Requirement                                                                                           |   |
|-------------------------------------------------------------------------------------------------------|---|
| vCenter object names do not contain forward slashes                                                   | ✓ |
| vSphere Powershell CLI 5 or later is installed on the Tidal Enterprise Orchestrator (TEO) server      |   |
| VMware Enterprise licensing is applied                                                                |   |
| VMware vSphere Distributed Resource Scheduler (DRS) is enabled                                        |   |
| VM templates have been created with VMware tools installed to support operating system customizations |   |

## Directory and Mail Server Requirements

For more information about these requirements, see [Directory and Mail Server Preparation, page 1-10](#).

**Table B-14** Requirements—Directory and Mail Server

| Requirement                                                                         |   |
|-------------------------------------------------------------------------------------|---|
| LDAP server is installed and configured, and Microsoft Active Directory is deployed | ✓ |
| SMTP server is installed and configured with an account to send and receive emails  |   |



## Organizations and Users Preparation

See [Organizations and Users Preparation, page 1-10](#).

**Table B-15** Requirements—Organizations and Users

| Requirement                                             |   |
|---------------------------------------------------------|---|
| Prepare a list of organizations                         | ✓ |
| Prepare a list of organization users                    |   |
| Prepare a list of Organization Technical Administrators |   |

## Create a Virtual Datacenter

**Table B-16** Requirements—Virtual Datacenter Creation

| Requirement                                       |   |
|---------------------------------------------------|---|
| vCenter platform element is registered            | ✓ |
| POD is created                                    |   |
| Register Datastores ( <a href="#">page 7-12</a> ) |   |
| Create networks ( <a href="#">page 8-21</a> )     |   |

## Create Shared Zones

**Table B-17** Requirements—Shared Zone Creation

| Requirement                                       |   |
|---------------------------------------------------|---|
| vCenter platform element is registered            | ✓ |
| POD is created                                    |   |
| Register Datastores ( <a href="#">page 7-12</a> ) |   |
| Create networks ( <a href="#">page 8-21</a> )     |   |

## Order VM From Template

**Table B-18** Requirements—Order VM from Template

| Requirement                                                     |   |
|-----------------------------------------------------------------|---|
| VM templates created and discovered                             | ✓ |
| Virtual Data Center or Shared Zone is created                   |   |
| Register Virtual Machine templates ( <a href="#">page 8-1</a> ) |   |

## Order a VM and Install an Operating System

**Table B-19** Requirements—Order a VM and Install an Operating System

| Requirement                                                                                            | ✓ |
|--------------------------------------------------------------------------------------------------------|---|
| VLAN for Cisco Server Provisioner to use as its private PXE VLAN defined in vCenter                    |   |
| Cisco Server Provisioner Operating System Template is created                                          |   |
| Virtual Data Center or Shared Zone is created                                                          |   |
| Register Cisco Server Provisioner Platform Element ( <a href="#">page 7-5</a> )                        |   |
| Create/Modify POD to contain the Cisco Server Provisioner Platform Element                             |   |
| Discover and Register Cisco Server Provisioner operating system templates ( <a href="#">page 8-2</a> ) |   |

## Order a Physical Server

**Table B-20** Requirements—Order a Physical Server

| Requirement                                                                                            | ✓ |
|--------------------------------------------------------------------------------------------------------|---|
| VLAN for Cisco Server Provisioner to use as its private PXE VLAN defined in UCS Manager                |   |
| At least one UCS service profile template for physical server provisioning is created                  |   |
| Cisco Server Provisioner Operating System Template is created                                          |   |
| Virtual Data Center or Shared Zone is created                                                          |   |
| Place blades in the Physical Blade Pool ( <a href="#">page 8-5</a> )                                   |   |
| Discover and register Cisco Server Provisioner operating system templates ( <a href="#">page 8-2</a> ) |   |
| Discover and register Cisco UCS service profile templates ( <a href="#">page 8-3</a> )                 |   |

## Provision ESXi

**Table B-21** Requirements—Provision ESXi

| Requirement                                                                                            | ✓ |
|--------------------------------------------------------------------------------------------------------|---|
| VLAN for Cisco Server Provisioner to use as its private PXE VLAN defined in UCS Manager                |   |
| At least one hypervisor UCS service profile template for each vCenter cluster is created               |   |
| Cisco Server Provisioner Operating System Template for ESXi is created                                 |   |
| Infrastructure Network is created ( <a href="#">page 8-21</a> )                                        |   |
| Place blades in the Virtual Blade Pool ( <a href="#">page 8-5</a> )                                    |   |
| Discover and register Cisco UCS service profile templates ( <a href="#">page 8-3</a> )                 |   |
| Discover and register Cisco Server Provisioner operating system templates ( <a href="#">page 8-2</a> ) |   |



# APPENDIX C

## Solution Deployment Checklists

---

To ensure full functionality of Cisco Intelligent Automation for Cloud (Cisco IAC), you must **strictly follow the setting up**, configuring, and deploying tasks that are presented in this guide in the sequence presented in this guide.

This appendix provides these checklists to aid you as you configure Cisco IAC:

- [Cisco Intelligent Automation for Cloud Prerequisites](#), page C-2
- [Tidal Enterprise Orchestrator Setup Checklist](#), page C-2
- [REX Adapter Installation Checklist](#), page C-2
- [Directory Integration Setup Checklist \(If Applicable\)](#), page C-3
- [Cloud Portal Setup Checklist](#), page C-3
- [Service Catalog Deployment Checklist](#), page C-4
- [Portal and Portlet Deployment Checklist](#), page C-4
- [Permissions Settings for Portal and Portlets Checklists](#), page C-5
- [Configure and Enable Approvals Checklist](#), page C-6
- [Configuration Wizard Checklist \(Optional\)](#), page C-7
- [Cloud Administration Setup Checklist](#), page C-8
- [Email Notification Template Modification Checklist](#), page C-9
- [Cloud Infrastructure Setup Checklist](#), page C-10
- [Organizations and Users Setup Checklist](#), page C-10
- [Directory Integration Setup Checklist \(If Applicable\)](#), page C-11



### Note

---

It is strongly recommended that as you configure Cisco IAC, you record the all of the settings you enter. Log the information in the worksheets in [Appendix D, “Solution Deployment Worksheets,”](#) and save them as a record that Cisco Services or administrators can consult should any problems arise.

---

# Cisco Intelligent Automation for Cloud Prerequisites

**Table C-1** Cisco Intelligent Automation for Cloud Prerequisites Checklist

| Task                                                                                                                                                                                                                                    |   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| You have reviewed <a href="#">Chapter 1, “Solution Prerequisites,”</a> completed the checklists in <a href="#">Appendix B, “Solution Prerequisites Checklists,”</a> and have confirmed that all of the Cisco IAC prerequisites are met. | ✓ |

## Tidal Enterprise Orchestrator Setup Checklist

For information and instructions, see [Chapter 2, “Configuring Cisco Tidal Enterprise Orchestrator and Deploying Cisco Intelligent Automation for Cloud Content.”](#)

**Table C-2** TEO Setup Checklist

| Task                                                                                                | See Page             |  |
|-----------------------------------------------------------------------------------------------------|----------------------|--|
| Import the Core Automation Pack                                                                     | <a href="#">2-3</a>  |  |
| Import the Common Activities Automation Pack                                                        | <a href="#">2-8</a>  |  |
| Import the Intelligent Automation for Compute Automation Pack                                       | <a href="#">2-9</a>  |  |
| Import the Intelligent Automation for Cloud Starter Automation Pack                                 | <a href="#">2-14</a> |  |
| Import the Intelligent Automation for Cloud Automation Pack                                         | <a href="#">2-21</a> |  |
| <i>(For Linux only)</i> Configure extended target properties for Cisco Cloud Portal Integration API | <a href="#">2-23</a> |  |
| <i>(For Linux only)</i> Configure extended target properties for Cisco Cloud Portal Request Center  | <a href="#">2-25</a> |  |
| Set up Internet Information Services                                                                | <a href="#">2-26</a> |  |
| Refresh TEO Server Web Service                                                                      | <a href="#">2-27</a> |  |

## REX Adapter Installation Checklist

For information and instructions, see [Chapter 3, “Installing the REX Adapter.”](#)

**Table C-3** REX Adapter Installation Checklist

| Task                    | See Page            |   |
|-------------------------|---------------------|---|
| Install the REX Adapter | <a href="#">3-1</a> | ✓ |

# Directory Integration Setup Checklist (If Applicable)


**Note**

These tasks are required **only** if external authentication is enabled for your environment. Otherwise, skip to the next checklist.

For information and instructions, see [Appendix A, “Setting Up Directory Integration.”](#)

**Table C-4**      *Directory Integration Setup Checklist*

| Task                                                             | See Page            | ✓ |
|------------------------------------------------------------------|---------------------|---|
| Verify that the prerequisites for directory integration are met  | <a href="#">A-2</a> |   |
| Configure the LDAP server                                        | <a href="#">A-3</a> |   |
| Configure authentication:                                        |                     |   |
| • Configure mappings                                             | <a href="#">A-5</a> |   |
| • Configure events                                               | <a href="#">A-6</a> |   |
| Configure authorization (Optional):                              |                     |   |
| • Create a security group for each user role on the LDAP server: |                     |   |
| – Cloud Provider Technical Administrator                         | <a href="#">A-8</a> |   |
| – Organization Technical Administrator                           | <a href="#">A-8</a> |   |
| – Virtual and Physical Server Owner                              | <a href="#">A-8</a> |   |
| – Virtual Server Owner                                           | <a href="#">A-8</a> |   |
| – Field Extender                                                 | <a href="#">A-8</a> |   |
| – Service Group                                                  | <a href="#">A-8</a> |   |
| • Add the nsAPI user to the Cloud Administration Group           | <a href="#">A-9</a> |   |
| • Configure user role mappings                                   | <a href="#">A-9</a> |   |
| Enable directory integration                                     | <a href="#">A-9</a> |   |

## Cloud Portal Setup Checklist

For information and instructions, see [Enable Web Services, page 4-2](#) and [Create a Dropbox for Data Synchronization, page 4-3](#).

**Table C-5**      *Cloud Portal Setup Checklist*

| Task                                      | See Page            | ✓ |
|-------------------------------------------|---------------------|---|
| Enable Web services                       | <a href="#">4-2</a> |   |
| Create a dropbox for data synchronization | <a href="#">4-3</a> |   |

# Service Catalog Deployment Checklist

For information and instructions, see [Import and Deploy Intelligent Automation for Cloud Service Catalogs](#), page 4-3

**Table C-6** *Service Catalog Deployment Checklist*

| Task                                              | See Page | ✓ |
|---------------------------------------------------|----------|---|
| Copy service catalog files to Cloud Portal server | 4-4      |   |
| Import and deploy service catalogs                | 4-4      |   |

# Portal and Portlet Deployment Checklist

For information and instructions, see [Import and Deploy Intelligent Automation for Cloud Service Catalogs](#), page 4-3

**Table C-7** *Portal Deployment and Configuration Checklist*

| Task                                                                                          | See Page | ✓ |
|-----------------------------------------------------------------------------------------------|----------|---|
| Copy portlets folder and extract files                                                        | 4-5      |   |
| Configure Cloud Portal stylesheets                                                            | 4-6      |   |
| Import and deploy portal pages                                                                | 4-8      |   |
| Modify maximum number of tabs, portals, and portlets                                          | 4-9      |   |
| Modify column settings for the Site Homepage                                                  | 4-11     |   |
| Set permissions for portal pages and portlets                                                 | 4-12     |   |
| Add portlet access to My Workspace                                                            | 4-17     |   |
| Add all user roles to the Cisco Intelligent Automation for Cloud Roles Group                  | 4-17     |   |
| Assign read/write permissions to Cloud Administrator for organization unit, person, and queue | 4-18     |   |
| Assign read/Write permissions to Cloud Administrator for role                                 | 4-18     |   |
| Assign permissions to Cloud Administrator for service queue management                        | 4-20     |   |

# Permissions Settings for Portal and Portlets Checklists

For information and instructions, see [Set Permissions for Portals and Portlets](#), page 4-12.

**Table C-8** *Permissions Settings for Portals Checklist*

| Task                            | See Page             | ✓ |
|---------------------------------|----------------------|---|
| Cloud Service Errors            | <a href="#">4-12</a> |   |
| Configuration Wizard            | <a href="#">4-12</a> |   |
| Manage Cloud Infrastructure     | <a href="#">4-12</a> |   |
| My Approvals                    | <a href="#">4-12</a> |   |
| My Orders                       | <a href="#">4-12</a> |   |
| My Servers                      | <a href="#">4-12</a> |   |
| My Virtual Data Centers         | <a href="#">4-12</a> |   |
| Network Management              | <a href="#">4-12</a> |   |
| Order Cloud Services            | <a href="#">4-12</a> |   |
| Organization Management         | <a href="#">4-12</a> |   |
| POD Resource Capacity           | <a href="#">4-12</a> |   |
| System Resource Capacity        | <a href="#">4-12</a> |   |
| System Resource Usage           | <a href="#">4-12</a> |   |
| System Setup                    | <a href="#">4-12</a> |   |
| Upgrade Wizard                  | <a href="#">4-12</a> |   |
| User Management                 | <a href="#">4-12</a> |   |
| Validate Platform Configuration | <a href="#">4-12</a> |   |
| VDC Calculator                  | <a href="#">4-12</a> |   |

**Table C-9** *Permissions Settings for Portlets Checklist*

| Task                                     | See Page             | ✓ |
|------------------------------------------|----------------------|---|
| <b>HTML:</b>                             |                      |   |
| CloudAdmin_OrgManagement                 | <a href="#">4-14</a> |   |
| CloudAdmin_SystemSetup                   | <a href="#">4-14</a> |   |
| Configuration_Wizard                     | <a href="#">4-14</a> |   |
| Homepage_Welcome                         | <a href="#">4-14</a> |   |
| OrderPage_KnowledgeCenter                | <a href="#">4-14</a> |   |
| OrderPage_OrderPhysicalandVirtualMachine | <a href="#">4-14</a> |   |
| OrderPage_OrderResource                  | <a href="#">4-14</a> |   |
| OrderPage_OrderVirtualMachine            | <a href="#">4-14</a> |   |
| OrgAdmin_UserManagement                  | <a href="#">4-14</a> |   |

**Table C-9** *Permissions Settings for Portlets Checklist (continued)*

| Task                           | See Page             | ✓ |
|--------------------------------|----------------------|---|
| Upgrade_Wizard                 | <a href="#">4-14</a> |   |
| VDC_Calculator                 | <a href="#">4-14</a> |   |
| <b>Javascript:</b>             |                      |   |
| BladePoolManagementPhysicalPie | <a href="#">4-14</a> |   |
| BladePoolManagementPie         | <a href="#">4-14</a> |   |
| CloudAdmin_ManageServiceItems  | <a href="#">4-14</a> |   |
| Infrastructure_Discovery       | <a href="#">4-14</a> |   |
| IPAMGroupFilterGrid            | <a href="#">4-14</a> |   |
| IPAMNetworkCapacity            | <a href="#">4-14</a> |   |
| Manage_MyErrorRemediations     | <a href="#">4-14</a> |   |
| Manage_MyServers               | <a href="#">4-14</a> |   |
| Manage_MyVDCs                  | <a href="#">4-14</a> |   |
| Physical_BCCapacityReport      | <a href="#">4-14</a> |   |
| Report_SystemResourceCapacity  | <a href="#">4-14</a> |   |
| Report_ViewCloudResourceUsage  | <a href="#">4-14</a> |   |
| Report_ViewPodCapacity         | <a href="#">4-14</a> |   |
| ServerOwner_ManageServiceItems | <a href="#">4-14</a> |   |
| Validate_PlatformConfiguration | <a href="#">4-14</a> |   |
| Virtual_ClusterCapacityReport  | <a href="#">4-14</a> |   |
| Virtual_DCCapacityColumnChart  | <a href="#">4-14</a> |   |

## Configure and Enable Approvals Checklist

For information and instructions, see [page 4-23](#).

**Table C-10** *Configure and Enable Approvals Checklist*

| Task                           | See Page             | ✓ |
|--------------------------------|----------------------|---|
| Configure and enable approvals | <a href="#">4-23</a> |   |



# Configuration Wizard Checklist (Optional)


**Note**

If you have opted **not** to use the Quick Setup Wizard, skip to [Cloud Administration Setup Checklist, page C-8](#).

After you have completed this checklist, you can skip the remaining checklists in this appendix.

For information and instructions, see [Chapter 5, “Running the Configuration Wizard.”](#) For information and instructions on individual tasks, see the page numbers provided in the checklist.

**Table C-11** Cisco IAC Quick Setup Wizard Checklist

| Task                                                                                  | See Page             | ✓ |
|---------------------------------------------------------------------------------------|----------------------|---|
| Step 1: Agent Properties Configuration                                                | <a href="#">5-4</a>  |   |
| • Create user accounts for both REX Agent and nsAPI users                             | <a href="#">6-2</a>  |   |
| • Set the username and password for “REX Set REX Agent Properties”                    | <a href="#">6-6</a>  |   |
| • Start the “REX Set REX Agent Properties” and “REX Set HTTP Agent Properties” agents | <a href="#">6-7</a>  |   |
| • Set the REX Agent Configuration properties                                          | <a href="#">6-7</a>  |   |
| • Set the HTTP Agent Configuration properties                                         | <a href="#">6-9</a>  |   |
| • Start all other agents                                                              | <a href="#">6-10</a> |   |
| Step 2: Cloud Administration                                                          | <a href="#">5-5</a>  |   |
| • Add Cloud Administration Organization                                               | <a href="#">6-15</a> |   |
| • Add Cloud Administrator                                                             | <a href="#">6-15</a> |   |
| • Add the nsAPI user as a Cloud Provider Technical Administrator                      | <a href="#">6-15</a> |   |
| • Assign Cloud Administration as the Home OU for the nsAPI user                       | <a href="#">6-2</a>  |   |
| Step 3: Connect Cloud Infrastructure                                                  | <a href="#">5-4</a>  |   |
| • Define the platform elements                                                        | <a href="#">7-2</a>  |   |
| Step 4: POD Management                                                                | <a href="#">5-4</a>  |   |
| • Create a POD                                                                        | <a href="#">7-11</a> |   |
| Step 5: Set System-wide Services and Provisioning Settings                            | <a href="#">5-4</a>  |   |
| • Set system-wide service options                                                     | <a href="#">7-7</a>  |   |
| • Set provisioning settings                                                           | <a href="#">7-6</a>  |   |
| • Stop and start all CIM agents                                                       | <a href="#">7-10</a> |   |
| Step 6: Add Networks                                                                  | <a href="#">5-4</a>  |   |
| • Add User or Community networks                                                      | <a href="#">8-21</a> |   |
| Step 7: Create Shared Zone                                                            | <a href="#">5-4</a>  |   |
| • Set up a shared zone server                                                         | <a href="#">7-13</a> |   |

# Cloud Administration Setup Checklist

For information and instructions, see [Chapter 6, “Creating Cloud Administration Organization and Administrative Accounts.”](#)

**Table C-12** *Cloud Administration Setup Checklist*

| Task                                                                                                                               | See Page             | ✓ |
|------------------------------------------------------------------------------------------------------------------------------------|----------------------|---|
| Configure and enable approvals                                                                                                     | <a href="#">4-23</a> |   |
| Set up REX and nsAPI user account                                                                                                  | <a href="#">6-2</a>  |   |
| Set username and password for REX Set REX agent properties                                                                         | <a href="#">6-6</a>  |   |
| Start REX Set REX Agent Property agent                                                                                             | <a href="#">6-7</a>  |   |
| Set REX Agent Configuration and verify that the agent properties are set correctly                                                 | <a href="#">6-7</a>  |   |
| Start REX Set HTTP Agent Property agent                                                                                            | <a href="#">6-8</a>  |   |
| Set HTTP Agent Configuration and verify that the agent properties are set correctly                                                | <a href="#">6-9</a>  |   |
| Start all other agents                                                                                                             | <a href="#">6-10</a> |   |
| Assign email addresses for queue notifications                                                                                     | <a href="#">6-10</a> |   |
| Modify the default email notification templates (see <a href="#">Table C-13 on page 9</a> for a checklist of all of the templates) | <a href="#">6-12</a> |   |
| Create the Cloud Provider Technical Administrator home organization                                                                | <a href="#">6-15</a> |   |
| Add the new user as a Cloud Administrator (no directory service)                                                                   | <a href="#">6-15</a> |   |

# Email Notification Template Modification Checklist

For information and instructions, see [Configure the Email Notification Templates, page 6-12](#).

**Table C-13** *Email Notification Templates Checklist*

| Email Template                                        | ✓ |
|-------------------------------------------------------|---|
| Add Role Completion Notification                      |   |
| Ad-Hoc Task Started                                   |   |
| Connection Cloud Platform Elements Completed Email    |   |
| CPO Error Notification Physical Server                |   |
| CPO Error Notification VM                             |   |
| Default Late Activity                                 |   |
| Failure to Create Network                             |   |
| Failure to Create Target Notification                 |   |
| Lease Expiration - First Warning                      |   |
| Lease Expiration - Second Warning                     |   |
| My Services Departmental Reviews                      |   |
| My Services Financial and Departmental Authorizations |   |
| My Services Service Group Reviews                     |   |
| Notification System Error in Service Request          |   |
| Order VM from Template Completion Notification        |   |
| Process Escalation                                    |   |
| Remove Role Completion Notification                   |   |
| Service Canceled Notification                         |   |
| Service Complete Notification                         |   |
| Service Confirmation Customer Acknowledgement         |   |
| Service Link Error on External Task                   |   |
| Service Rejected Notification                         |   |
| Service Started Email                                 |   |
| Task Fulfillment Escalation Notification              |   |
| Task Fulfillment Pending Notification                 |   |
| Tenant Management Complete Notification               |   |

# Cloud Infrastructure Setup Checklist

For information and instructions, see [Chapter 7, “Setting Up the Cloud Infrastructure.”](#)

**Table C-14** *Cloud Infrastructure Setup Checklist*

| Task                                                 | See Page             | ✓ |
|------------------------------------------------------|----------------------|---|
| Define the VMware vCenter Server platform element    | <a href="#">7-2</a>  |   |
| Define the Cisco UCS Manager platform element        | <a href="#">7-3</a>  |   |
| Define the Cisco Server Provisioner platform element | <a href="#">7-5</a>  |   |
| Set provisioning settings                            | <a href="#">7-6</a>  |   |
| Add infrastructure network                           | <a href="#">8-21</a> |   |
| Add community network                                | <a href="#">8-21</a> |   |
| Create one or more PODs                              | <a href="#">7-11</a> |   |
| Set up the shared zone                               | <a href="#">7-13</a> |   |

# Organizations and Users Setup Checklist

For information and instructions, see [Chapter 9, “Setting Up an Organization and Adding Users.”](#)

**Table C-15** *Organizations and Users Setup Checklist*

| Task                                                                               | See Page             | ✓ |
|------------------------------------------------------------------------------------|----------------------|---|
| Create an organization                                                             | <a href="#">9-2</a>  |   |
| Create a new user to add as an Organization Technical Administrator                | <a href="#">9-3</a>  |   |
| Assign read/write permissions for Role—Organization Technical Administrator        | <a href="#">4-22</a> |   |
| Assign read/write permissions for Person—Organization Technical Administrator role | <a href="#">4-22</a> |   |
| Assign read/write permissions for Person—Server Owner roles                        | <a href="#">4-23</a> |   |
| Add a Server Owner                                                                 | <a href="#">9-4</a>  |   |

# Directory Integration Setup Checklist (If Applicable)


**Note**

These tasks are required **only** if external authentication is enabled for your environment. Otherwise, skip to the next checklist.

For information and instructions, see [Appendix A, “Setting Up Directory Integration.”](#)

**Table C-16**      *Directory Integration Setup Checklist*

| Task                                                                                                     | See Page | ✓ |
|----------------------------------------------------------------------------------------------------------|----------|---|
| Set up directory structure on the LDAP server, with Groups and Users folders.                            |          |   |
| Create the nsAPI user account on the LDAP server.                                                        |          |   |
| Create the lookup user account with “Read MemberOf” lookup permissions.                                  |          |   |
| Configure the LDAP server in Cloud Portal.                                                               |          |   |
| Configure authentication:                                                                                |          |   |
| • Configure mappings.                                                                                    |          |   |
| • Configure events.                                                                                      |          |   |
| Configure authorization ( <i>Optional</i> ):                                                             |          |   |
| • Create security groups for all six Cloud Portal user roles in each “Groups” folder on the LDAP server. |          |   |
| • Add the nsAPI user to the Cloud Portal Technical Administrator security group.                         |          |   |
| • Configure user role mappings.                                                                          |          |   |
| Enable directory integration.                                                                            |          |   |

■ Directory Integration Setup Checklist (If Applicable)



# APPENDIX D

## Solution Deployment Worksheets

---

Use the worksheets provided in this appendix to keep a current record of your settings. Update the worksheets periodically for administration changes and for accuracy when diagnosing problems that might arise.

This appendix provides the following worksheets:

- [Hardware Specifications, page D-2](#)
- [Software Specifications, page D-3](#)
- [Database Connection Settings, page D-4](#)
- [TEO Web Service Target Settings, page D-5](#)
- [TEO-Cloud Portal Integration API Connection User Account Credentials, page D-5](#)
- [Cisco Service Portal Request Center and Service Link User Account Credentials, page D-5](#)
- [REX Adapter Installation Settings, page D-6](#)
- [Directory Integration Settings \(If Applicable\), page D-7](#)
- [Cloud Administrator and Organization Settings, page D-9](#)
- [Agent Properties Settings, page D-9](#)
- [Email Addresses for Queue Notifications, page D-11](#)
- [Cloud Platform Connection Settings, page D-11](#)
- [Provisioning Settings, page D-13](#)
- [System-wide Service Options, page D-13](#)
- [Network Settings, page D-14](#)
- [POD Settings, page D-14](#)
- [Shared Zone Settings, page D-15](#)
- [Standards Settings \(Optional\), page D-15](#)

# Hardware Specifications

For minimum requirements for hardware components, see [Minimum Hardware Requirements for Platform Elements, page 1-2](#).

**Table D-1** *Hardware Specifications for Platform Elements*

| Platform Element         | Component  | Client | Server |
|--------------------------|------------|--------|--------|
| TEO Server               | CPU        |        |        |
|                          | Memory     |        |        |
|                          | Disk space |        |        |
| Cloud Portal             | CPU        | —      |        |
|                          | Memory     | —      |        |
|                          | Disk space | —      |        |
| Cloud Portal Database    | CPU        | —      |        |
|                          | Memory     | —      |        |
|                          | Disk space | —      |        |
| Cisco Server Provisioner | CPU        | —      |        |
|                          | Memory     | —      |        |
|                          | Disk space | —      |        |
| UCS                      | CPU        | —      |        |
|                          | Memory     | —      |        |
|                          | Blades     | —      |        |



# Software Specifications

For minimum requirements for software components, see [Minimum Software Requirements, page 1-3](#).

**Table D-2** Minimum Software Requirements

| Component                           | Server                                                                                                            | Version |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------|---------|
| Application Server Operating System | TEO                                                                                                               |         |
|                                     | Cloud Portal                                                                                                      |         |
|                                     | Cisco Server Provisioner                                                                                          |         |
| Application Server Framework        | TEO                                                                                                               |         |
|                                     | Cloud Portal                                                                                                      |         |
| Application Software                | TEO                                                                                                               |         |
|                                     | Cloud Portal                                                                                                      |         |
| LDAP Server                         | TEO                                                                                                               |         |
|                                     | Cloud Portal                                                                                                      |         |
|                                     | <b>Note</b> LDAP server requirements apply only if your environment has been enabled for external authentication. |         |
| Web server                          | TEO                                                                                                               |         |
|                                     | Cloud Portal                                                                                                      |         |
| Database                            | TEO                                                                                                               |         |
|                                     | Cloud Portal                                                                                                      |         |
| Web browser                         | TEO                                                                                                               |         |
|                                     | Cloud Portal                                                                                                      |         |
| Virtualization                      | Hypervisor                                                                                                        |         |
|                                     | Hypervisor Manager                                                                                                |         |
| Physical Server Provisioning        | Cisco UCS Manager                                                                                                 |         |

# Database Connection Settings

*Table D-3 Database Connection Settings*

| Component                        | Server                              | Version |
|----------------------------------|-------------------------------------|---------|
| Database Specifications          | Type (Oracle or Microsoft SQL)      |         |
|                                  | Version                             |         |
|                                  | Host                                |         |
|                                  | Port                                |         |
| TEO credentials                  | Database or Windows authentication? |         |
|                                  | Username                            |         |
|                                  | Password                            |         |
|                                  | Domain                              |         |
| RequestCenter credentials        | Database or Windows authentication? |         |
|                                  | Username                            |         |
|                                  | Password                            |         |
|                                  | Domain                              |         |
| Datamart credentials             | Database or Windows authentication? |         |
|                                  | Username                            |         |
|                                  | Password                            |         |
|                                  | Domain                              |         |
| Cisco Service Portal credentials | Database or Windows authentication? |         |
|                                  | Username                            |         |
|                                  | Password                            |         |
|                                  | Domain                              |         |

## TEO Web Service Target Settings

TEO web service settings are configured when the Cisco Intelligent Automation for Cloud Compute Automation Pack is imported into TEO. (See [page 2-9](#).)

**Table D-4** TEO Default Web Service Target Settings

| Requirement                                                                                                                    | Setting |
|--------------------------------------------------------------------------------------------------------------------------------|---------|
| HTTP Port of the TEO web service target                                                                                        |         |
| HTTPS or HTTP authentication mechanism (NTLM, Digest, or Basic)                                                                |         |
| Web service target credentials:                                                                                                |         |
| <ul style="list-style-type: none"> <li>Domain of user account that is used to connect to the TEO Web service target</li> </ul> |         |
| <ul style="list-style-type: none"> <li>User account username</li> </ul>                                                        |         |
| <ul style="list-style-type: none"> <li>User account password</li> </ul>                                                        |         |

## TEO-Cloud Portal Integration API Connection User Account Credentials

The user credentials for the Cloud Portal Integration API Connection to TEO are created when the Intelligent Automation for Cloud Starter Automation Pack is imported into TEO. (See [page 2-14](#).) This user account is referred to as the *nsAPI user account*.

**Table D-5** TEO-Cloud Portal Integration API Connection User Account Credentials

| Requirement | Setting |
|-------------|---------|
| Username    |         |
| Password    |         |

## Cisco Service Portal Request Center and Service Link User Account Credentials

For instructions, see [Import and Configure the Intelligent Automation for Cloud Automation Pack, page 2-21](#).

**Table D-6** Cisco Service Portal Request Center and Service Link User Account Credentials

| Requirement | Setting |
|-------------|---------|
| Username    |         |
| Password    |         |

# REX Adapter Installation Settings

Record the settings using the worksheet provided for your database server.

For information and instructions, see [Chapter 3, “Installing the REX Adapter.”](#)

**Table D-7** REX Adapter Installation Settings—SQL Server

| Variable | Definition |
|----------|------------|
| DBSERVER |            |
| DBPORT   |            |
| DBNAME   |            |
| DBUSER   |            |
| DBPW     |            |

**Table D-8** REX Adapter Installation Settings—Oracle® Database (Windows or Linux)

| Variable | Definition |
|----------|------------|
| DBSERVER |            |
| DBPORT   |            |
| SID      |            |
| DBUSER   |            |
| DBPWD    |            |

# Directory Integration Settings (If Applicable)

For information, instructions, and an example of directory integration, see [Appendix A, “Setting Up Directory Integration.”](#)

- [LDAP Server Configurations, page D-7](#)
- [Mappings Settings, page D-8](#)
- [Events Settings, page D-8](#)

## LDAP Server Configurations

For information and instructions, see [Step 1: Configuring the LDAP Server, page A-3](#).

**Table D-9** Directory Integration—LDAP Server Settings

| Requirement                                | Setting |
|--------------------------------------------|---------|
| Datasource name                            |         |
| Datasource description ( <i>optional</i> ) |         |
| Protocol                                   |         |
| Server product and version                 |         |
| BindDN                                     |         |
| Host                                       |         |
| User BaseDN                                |         |
| Port number                                |         |
| Password                                   |         |

## Configure Authentication

### Configure Mapping

For information and instructions, see [Configure Mappings, page A-5](#).

**Table D-10** Directory Integration—Mapping Configurations

| Requirement                             | Setting/Mapping Attribute |
|-----------------------------------------|---------------------------|
| Mapping name                            |                           |
| Mapping description ( <i>optional</i> ) |                           |
| Person data:                            |                           |
| • First Name                            |                           |
| • Last Name                             |                           |
| • Login ID                              |                           |
| • Personal Identification               |                           |

**Table D-10** Directory Integration—Mapping Configurations (continued)

| Requirement              | Setting/Mapping Attribute |
|--------------------------|---------------------------|
| • Email Address          |                           |
| • Home Organization Unit |                           |
| • Password               |                           |

## Configure Events

For information and instructions, see [Configure Mappings, page A-5](#).

**Table D-11** Directory Integration—Event Configurations

| Requirement | Setting |
|-------------|---------|
| EUABindDN   |         |

## Mappings Settings

For information and instructions, see [Configure Mappings, page A-5](#).

**Table D-12** Directory Integration—Mappings Settings

| Requirement            | Setting |
|------------------------|---------|
| First name             |         |
| Last name              |         |
| Login ID               |         |
| Person identification  |         |
| Email address          |         |
| Home organization unit |         |
| Password               |         |
| Role list              |         |

## Events Settings

For information and instructions, see [Configure Events, page A-6](#).

**Table D-13** Directory Integration—Events Settings

| Requirement | Setting |
|-------------|---------|
| EUABindDN   |         |

# Cloud Administrator and Organization Settings

For instructions, see [Chapter 6, “Creating Cloud Administration Organization and Administrative Accounts.”](#)

**Table D-14** Cloud Administrator and Organization Settings

| Requirement                          | Setting                       |                                                                                                      |
|--------------------------------------|-------------------------------|------------------------------------------------------------------------------------------------------|
| nsAPI user credentials:              | Username                      | See <a href="#">TEO-Cloud Portal Integration API Connection User Account Credentials</a> , page D-5. |
|                                      | Password                      |                                                                                                      |
|                                      | Current role assigned         |                                                                                                      |
|                                      | Current organization assigned |                                                                                                      |
| REX adapter user credentials         | Username                      |                                                                                                      |
|                                      | Password                      |                                                                                                      |
|                                      | Current role assigned         |                                                                                                      |
|                                      | Current organization assigned |                                                                                                      |
| Cloud Administrator—Organization     | Organization name             |                                                                                                      |
| Cloud Administrator—User credentials | Username                      |                                                                                                      |
|                                      | Password                      |                                                                                                      |
|                                      | Current role assigned         |                                                                                                      |
|                                      | Current organization assigned |                                                                                                      |

## Agent Properties Settings

For information and instructions, see [Configure Agent Properties](#), page 6-5.

- [REX Set REX Agent Configuration Settings](#), page D-9
- [REX Agent Configuration Settings](#), page D-10
- [Set HTTP Properties Configuration Settings](#), page D-10

## REX Set REX Agent Configuration Settings

For more instructions, see [Set Username and Password for REX Set REX Agent Properties](#), page 6-6.

**Table D-15** REX Set REX Agent Properties Settings

| Requirement                            | Setting |
|----------------------------------------|---------|
| REXOutboundAdapter.Username - Username |         |
| REXOutboundAdapter.Password - Password |         |

## REX Agent Configuration Settings

For more instructions, see [Set REX Agent Configuration](#), page 6-7.

*Table D-16 REX Set REX Agent Properties Settings*

| Requirement  | Setting |
|--------------|---------|
| REX username |         |
| REX password |         |

## Set HTTP Properties Configuration Settings

For more instructions, see [Set HTTP Agent Configuration](#), page 6-9.

*Table D-17 HTTP Agent Settings*

| Requirement                           | Setting |
|---------------------------------------|---------|
| Process Orchestrator hostname         |         |
| Authentication Scheme (NTLM or Basic) |         |
| Process Orchestrator username         |         |
| Process Orchestrator password         |         |
| Process Orchestrator domain           |         |
| Cloud Portal hostname                 |         |



# Email Addresses for Queue Notifications

For instructions, see [Configure the Email Notification Templates](#), page 6-12.

**Table D-18** *Email Addresses for Queue Notifications*

| Queue                              | Email Address(es) |
|------------------------------------|-------------------|
| Default Service Delivery           |                   |
| Cloud Service Cancellation         |                   |
| Cloud Service Delivery Management  |                   |
| Cloud Service Lease Administration |                   |
| Cloud Service Remediation          |                   |

## Cloud Platform Connection Settings

For instructions, see [Connect the Cloud Platform Elements](#), page 7-2.

- [VMware vCenter Server Connection Settings](#)
- [Cisco UCS Manager Connection Settings](#)
- [Cisco Server Provisioner Connection Settings](#)

## VMware vCenter Server Connection Settings

For instructions, see [Define the VMware vCenter Server Platform Element](#), page 7-2.

**Table D-19** *VMware vCenter Server Connection Settings*

| Platform Element      | Requirement                          | Setting |
|-----------------------|--------------------------------------|---------|
| VMware vCenter Server | Host name                            |         |
|                       | Port                                 |         |
|                       | Secure connection protocol?<br>(T/F) |         |
|                       | Username                             |         |
|                       | Password                             |         |

## Cisco UCS Manager Connection Settings

For instructions, see [Define the Cisco UCS Manager Platform Element, page 7-3](#).

**Table D-20** Cisco UCS Manager Connection Settings

| Platform Element  | Requirement                       | Setting |
|-------------------|-----------------------------------|---------|
| Cisco UCS Manager | Host name                         |         |
|                   | Port                              |         |
|                   | Secure connection protocol? (T/F) |         |
|                   | Ignore certificate error? (T/F)   |         |
|                   | Time zone                         |         |
|                   | Username                          |         |
|                   | Password                          |         |

## Cisco Server Provisioner Connection Settings

For instructions, see [Define the Cisco Server Provisioner Platform Element, page 7-5](#).

**Table D-21** Cisco Server Provisioner Connection Settings

| Platform Element         | Requirement    | Setting |
|--------------------------|----------------|---------|
| Cisco Server Provisioner | Host name      |         |
|                          | Port           |         |
|                          | Username       |         |
|                          | Password       |         |
|                          | Device user ID |         |

# Provisioning Settings

For instructions, see [Set Provisioning Settings, page 7-6](#).

**Table D-22** *Provisioning Settings*

| Requirement                                                       | Setting |
|-------------------------------------------------------------------|---------|
| Cisco SP time zone                                                |         |
| Default virtual server clone timeout                              |         |
| Cloud duplicate alert suppression time period                     |         |
| Cloud Domain                                                      |         |
| Cloud Domain User                                                 |         |
| Cloud Domain Password                                             |         |
| Cloud Default Time Zone Linux                                     |         |
| Cloud Default Time Zone Windows                                   |         |
| Cisco Cloud Portal Data Synchronization<br>Dropbox Base Directory |         |
| Cisco Cloud Portal Drop Input Location                            |         |
| Cisco Cloud Portal Drop Backup Location                           |         |
| Cisco Cloud Portal Drop Temp Location                             |         |

# System-wide Service Options

For instructions, see [Set System-wide Service Options, page 7-7](#).

**Table D-23** *System-wide Service Options*

| Name                                    | Setting |
|-----------------------------------------|---------|
| Virtual Machine From Template Ordering  |         |
| Virtual Machine and Install OS Ordering |         |
| Physical Server Ordering                |         |
| ESXi Provisioning                       |         |
| Shared Zone Ordering                    |         |
| Virtual Data Center Ordering            |         |
| Optional Customer Message               |         |

# Network Settings

For instructions about adding infrastructure, community, user, or management networks, see [Add Additional Networks](#), page 8-21.

**Table D-24** <network\_type> Network Settings

| Requirement                                                  | Setting |
|--------------------------------------------------------------|---------|
| Network name                                                 |         |
| Subnet address specification (IP address/<br>routing prefix) |         |
| Community network                                            |         |
| Public network                                               |         |
| Network type                                                 |         |
| NetworksSource                                               |         |
| vCenter portgroup                                            |         |
| UCS VLAN                                                     |         |
| Subnet mask                                                  |         |
| Gateway address (if other than default)                      |         |
| FHRP1 address                                                |         |
| FHRP2 address                                                |         |
| Broadcast address (if other than default)                    |         |
| Primary DNS address                                          |         |
| Secondary DNS address                                        |         |

# POD Settings

For instructions, see [Create One or More PODs](#), page 7-11.

**Table D-25** Shared Zone Settings

| Requirement                       | Setting |
|-----------------------------------|---------|
| Name                              |         |
| Description                       |         |
| VMware vCenter Instance           |         |
| VMware Datacenter                 |         |
| Cisco UCS Manager Instance        |         |
| Cisco Server Provisioner Instance |         |

# Shared Zone Settings

For instructions, see [Set Up a Shared Zone, page 7-13](#).

**Table D-26** Shared Zone Settings

| Requirement               | Setting |
|---------------------------|---------|
| POD                       |         |
| VMware vCenter Datacenter |         |

## Standards Settings (Optional)

Modifying standards settings for service options is optional, but it is recommended for the following:

- [Lease Term Standards](#)
- [Operating Systems Standards](#)
- [Server Size Standards](#)
- [VDC Size Standards](#)

If you have opted not to modify any standards settings for these service options, check the following check box:

**No standard settings have been modified from the default values.**

## Lease Term Standards

If you added new lease terms, record the information in [Table D-27](#). If you have not added new lease terms, check the check box below.

For instructions, see [Add, Modify, or Delete a Lease Term Standard, page 8-8](#).

**Lease term standards have not been modified from the default values.**

**Table D-27** Lease Term Settings

| Template           | Requirement                        | Settings |
|--------------------|------------------------------------|----------|
| New lease duration | Lease term (for example, 6 months) |          |
|                    | Runtime (seconds)                  |          |
|                    | Storage (seconds)                  |          |
|                    | Warning 1 (seconds)                |          |

Table D-27 Lease Term Settings (continued)

| Template           | Requirement                        | Settings |
|--------------------|------------------------------------|----------|
| New lease duration | Lease term (for example, 6 months) |          |
|                    | Runtime (seconds)                  |          |
|                    | Storage (seconds)                  |          |
|                    | Warning 1 (seconds)                |          |
| New lease duration | Lease term (for example, 6 months) |          |
|                    | Runtime (seconds)                  |          |
|                    | Storage (seconds)                  |          |
|                    | Warning 1 (seconds)                |          |
| New lease duration | Lease term (for example, 6 months) |          |
|                    | Runtime (seconds)                  |          |
|                    | Storage (seconds)                  |          |
|                    | Warning 1 (seconds)                |          |

## Operating Systems Standards

For instructions, see [Add, Modify, or Delete an Operating System Standard](#), page 8-11.

No operating systems standards have been added or modified.

Table D-28 Operating System Standards Settings

| OS Type (Windows, Linux, ESXi)        | OS System |
|---------------------------------------|-----------|
| Linux                                 |           |
| Windows                               |           |
| ESXi                                  |           |
| New operating system standard—OS Type |           |
| New operating system standard—OS Type |           |
| New operating system standard—OS Type |           |

## Server Size Standards

For instructions, see [Add, Modify, or Delete a Server Size Standard](#), page 8-13.

No server size standards have been added or modified.

**Table D-29** Server Size Standards Settings

| Size Label                          | Component    | Setting |
|-------------------------------------|--------------|---------|
| Small                               | CPUs         |         |
|                                     | Memory (GB)  |         |
|                                     | Storage (GB) |         |
| Medium                              | CPUs         |         |
|                                     | Memory (GB)  |         |
|                                     | Storage (GB) |         |
| Large                               | CPUs         |         |
|                                     | Memory (GB)  |         |
|                                     | Storage (GB) |         |
| New server size standard (optional) | Size label   |         |
|                                     | CPUs         |         |
|                                     | Memory (GB)  |         |
|                                     | Storage (GB) |         |
| New server size standard (optional) | Size label   |         |
|                                     | CPUs         |         |
|                                     | Memory (GB)  |         |
|                                     | Storage (GB) |         |
| New server size standard (optional) | Size label   |         |
|                                     | CPUs         |         |
|                                     | Memory (GB)  |         |
|                                     | Storage (GB) |         |

## VDC Size Standards

For instructions, see [Add, Modify, or Delete a VDC Size Standard](#), page 8-15.

No VDC size standards have been added or modified.

*Table D-30 VDC Size Standards Settings*

| Size Label | Component                             | Setting |
|------------|---------------------------------------|---------|
| Small      | Maximum virtual servers               |         |
|            | Maximum vCPU                          |         |
|            | Maximum memory (GB)                   |         |
|            | Maximum total storage (GB)            |         |
|            | Maximum physical servers              |         |
|            | CPU limit (MHz)                       |         |
|            | Resource pool CPU reservation (MHz)   |         |
|            | Resource pool memory reservation (GB) |         |
|            | Number of snapshots                   |         |
|            | VDC                                   |         |
| Medium     | Maximum virtual servers               |         |
|            | Maximum vCPU                          |         |
|            | Maximum memory (GB)                   |         |
|            | Maximum total storage (GB)            |         |
|            | Maximum physical servers              |         |
|            | CPU limit (MHz)                       |         |
|            | Resource pool CPU reservation (MHz)   |         |
|            | Resource pool memory reservation (GB) |         |
|            | Number of snapshots                   |         |
|            | VDC                                   |         |



Table D-30 VDC Size Standards Settings (continued)

| Size Label                       | Component                             | Setting |
|----------------------------------|---------------------------------------|---------|
| Large                            | Maximum virtual servers               |         |
|                                  | Maximum vCPU                          |         |
|                                  | Maximum memory (GB)                   |         |
|                                  | Maximum total storage (GB)            |         |
|                                  | Maximum physical servers              |         |
|                                  | CPU limit (MHz)                       |         |
|                                  | Resource pool CPU reservation (MHz)   |         |
|                                  | Resource pool memory reservation (GB) |         |
|                                  | Number of snapshots                   |         |
|                                  | VDC                                   |         |
| New VDC size standard (optional) | Maximum virtual servers               |         |
|                                  | Maximum vCPU                          |         |
|                                  | Maximum memory (GB)                   |         |
|                                  | Maximum total storage (GB)            |         |
|                                  | Maximum physical servers              |         |
|                                  | CPU limit (MHz)                       |         |
|                                  | Resource pool CPU reservation (MHz)   |         |
|                                  | Resource pool memory reservation (GB) |         |
|                                  | Number of snapshots                   |         |
|                                  | VDC                                   |         |
| New VDC size standard (optional) | Maximum virtual servers               |         |
|                                  | Maximum vCPU                          |         |
|                                  | Maximum memory (GB)                   |         |
|                                  | Maximum total storage (GB)            |         |
|                                  | Maximum physical servers              |         |
|                                  | CPU limit (MHz)                       |         |
|                                  | Resource pool CPU reservation (MHz)   |         |
|                                  | Resource pool memory reservation (GB) |         |
|                                  | Number of snapshots                   |         |
|                                  | VDC                                   |         |

*Table D-30 VDC Size Standards Settings (continued)*

| Size Label                       | Component                             | Setting |
|----------------------------------|---------------------------------------|---------|
| New VDC size standard (optional) | Maximum virtual servers               |         |
|                                  | Maximum vCPU                          |         |
|                                  | Maximum memory (GB)                   |         |
|                                  | Maximum total storage (GB)            |         |
|                                  | Maximum physical servers              |         |
|                                  | CPU limit (MHz)                       |         |
|                                  | Resource pool CPU reservation (MHz)   |         |
|                                  | Resource pool memory reservation (GB) |         |
|                                  | Number of snapshots                   |         |
|                                  | VDC                                   |         |



## I N D E X

---

### A

#### Active Directory

integration configuration examples [A-1 to A-9](#)

#### agents

CIM file [6-5](#)

configuring HTTP agents [6-9](#)

configuring REX agents [6-7](#)

REX Set HTTP Agent Properties [6-7](#)

REX Set REX Agent Properties [6-6, 6-7](#)

starting [6-10](#)

application server framework, software requirements for [1-3](#)

application software, requirements for [1-3](#)

authorization (directory integration), configuring [A-8 to A-9](#)

automation pack import wizard [2-2 to 2-20, ?? to 2-22](#)

automation pack import wizard (TEO) [2-2](#)

#### automation packs

importing Common Activities automation pack [2-8](#)

importing Core automation pack [2-3, 2-7](#)

importing Intelligent Automation for Cloud Starter automation pack [2-14, 2-22](#)

importing Intelligent Automation for Compute automation pack [2-9, 2-13, 2-20](#)

using the automation pack import wizard [2-22](#)

---

### C

#### Cisco Cloud Portal

hardware requirements [1-2](#)

Cisco IAC Starter Edition Administration portals, setting permissions for [4-12](#)

#### Cisco Server Provisioner

defining as platform element [7-5](#)

Cisco Server Provisioner, hardware requirements for [1-2](#)

#### Cisco UCS Manager

defining as platform element [7-3](#)

#### Cloud Portal

configuring Cloud Portal stylesheets

Cloud Portal database, hardware requirements for [1-2](#)

#### Cloud Provider Technical Administrator

adding [6-15](#)

creating home organization for [6-15](#)

column settings. modifying on Site Homepage [4-11](#)

Common Activities automation pack, importing in TEO [2-8](#)

Core automation pack, importing in TEO [2-3, 2-7](#)

---

### D

#### database

Cloud Portal database, hardware requirements for [1-2](#)

database server, software requirements for [1-3](#)

#### data synchronization

creating dropbox for [4-3](#)

#### directory integration

adding nsAPI user to Cloud Administrator security group [A-9](#)

configuring [?? to A-9](#)

configuring authentication [A-5 to A-7](#)

configuring authorization [A-8 to A-9](#)

configuring events [A-6](#)

configuring mappings [A-5](#)

configuring user role mappings [A-9](#)

creating security groups for roles [A-8](#)

examples in Active Directory [A-1 to A-9](#)

Optional Person Data Mappings [A-9](#)

dropbox, creating [4-3](#)

---

**E**

email notifications

- configuring templates [6-12](#)
- for service queues [6-10](#)

events, configuring (directory integration) [A-6](#)

---

**H**

HTTP agents, configuring [6-9](#)

---

**I**

importing

- automation packs [2-2 to 2-22](#)
- Common Activities automation pack [2-8](#)
- Core automation pack [2-3](#)
- Intelligent Automation for Cloud Starter automation pack [2-14](#)
- Intelligent Automation for Compute automation pack [2-9](#)

Intelligent Automation for Cloud Starter automation pack, importing in TEO [2-14, 2-22](#)

Intelligent Automation for Compute automation pack, importing in TEO [2-9, 2-13, 2-20](#)

---

**L**

LDAP server, software requirements for [1-3](#)

---

**M**

mappings, configuring (directory integration) [A-5](#)

Microsoft SQL Server, requirements for [1-3](#)

---

**N**

nsAPI user account

- setting up [6-2](#)

---

**O**

operating system

- templates [8-1](#)

Oracle Database server, requirements for [1-3](#)

organizations

- Cloud Administrator home organization, creating [6-15](#)

---

**P**

permissions

- for service queue management [4-20](#)
- portlets [4-14](#)
- read/write for organization units [4-17](#)
- read/write for person [4-17](#)
- read/write for queues [4-17](#)
- read/write for role [4-18](#)

person data, configuring (directory integration) [A-5](#)

platform elements

- Cisco Server Provisioner, defining [7-5](#)
- Cisco UCS Manager, defining [7-3](#)
- connecting [7-2 to ??](#)
- VMware vCenter Server, defining [7-2](#)

portal packages, importing and deploying [4-5 to 4-9](#)

portlets

- setting permissions for [4-14](#)

Prerequisites, IAC [1-1](#)

provisioning settings, configuring [7-6](#)

---

**Q**

queues

- read/write permissions for [4-17](#)

---

**R**

requirements

- application software [1-3](#)

Cisco Cloud Portal (hardware) [1-2](#)  
 Cisco Server Provisioner (hardware) [1-2](#)  
 Cloud Portal database (hardware) [1-2](#)  
   database server (software) [1-3](#)  
   hardware [1-3](#)  
   LDAP server (software) [1-3](#)  
   platform elements (hardware) [1-2](#)  
   web server (software) [1-3](#)  
 requirements, software  
   application server framework [1-3](#)  
 REX adapter  
   installing [3-1](#)  
   prerequisites for installation [3-2](#)  
 REX agents, configuring [6-7](#)  
 REX Set HTTP Agent Properties  
   starting [6-7](#)  
 REX Set REX Agent Properties  
   setting username and password for [6-6](#)  
   starting [6-7](#)  
 REX user account [6-2](#)

---

**S**

security groups  
   adding nsAPI user (directory integration) [A-9](#)  
   creating (directory integration) [A-8](#)  
 server templates [8-1](#)  
 service queues  
   assigning email addresses for notifications [6-10](#)  
   setting permissions for [4-20](#)  
 shared zone, configuring [7-13](#)  
 software requirements  
   application server framework [1-3](#)  
   application software [1-3](#)  
   database server [1-3](#)  
   LDAP server [1-3](#)  
   web server [1-3](#)  
 SQL Server, requirements for [1-3](#)  
 Starter Edition Quick Setup Wizard [5-1 to 5-11](#)

stylesheets. *See* Cloud Portal stylesheets  
 system requirements [1-2](#)

---

## T

tap files. *See* automation packs  
 templates [8-1](#)  
   for email notifications [6-12](#)  
 TEO  
   configuring [?? to 2-27](#)

---

## U

UCS service profile templates [8-1](#)

---

## V

vCenter Server, defining as platform element [7-2](#)  
 virtual servers  
   templates [8-1](#)  
 VMware  
   vCenter Server, defining as platform element [7-2](#)

---

## W

web server, software requirements for [1-3](#)  
 web services, enabling [4-2](#)  
 wizard  
   automation pack import wizard (TEO) [2-2](#)  
   Starter Edition Quick Setup Wizard [5-1 to 5-11](#)

