Cisco Intelligent Automation for Cloud Configuration Guide

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

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

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

INDEX

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

Note Means *reader take note*.

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

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

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

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

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 **Note** LDAP Server requirements only apply if you are using a directory service to import user and organization information.	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, VMware[1] 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 STMP 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

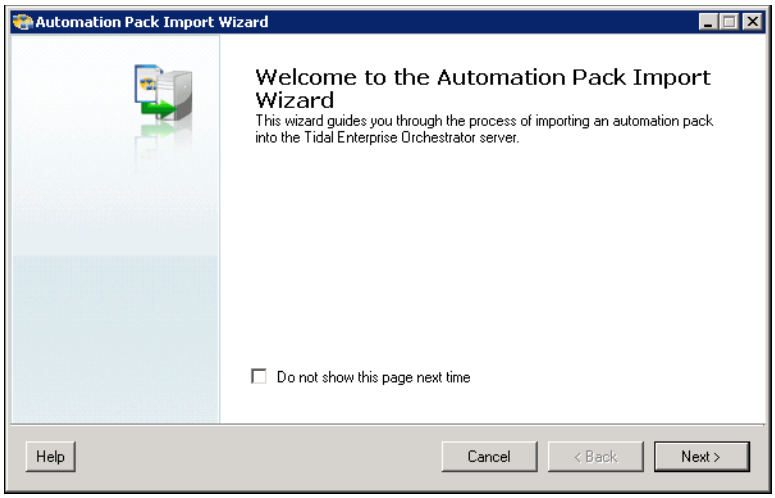
Step 3 Proceed to Import the Core Automation Pack.

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.

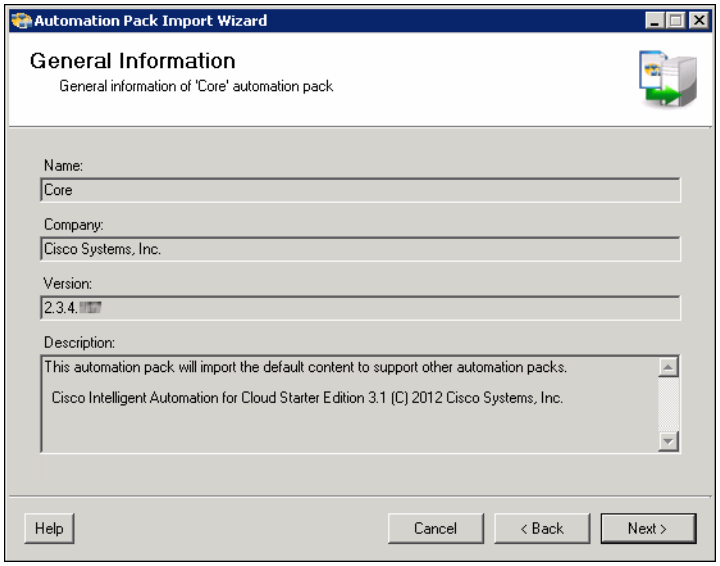
Step 1 On the Welcome to the Automation Pack Import Wizard panel, review the information, then click **Next**.

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.

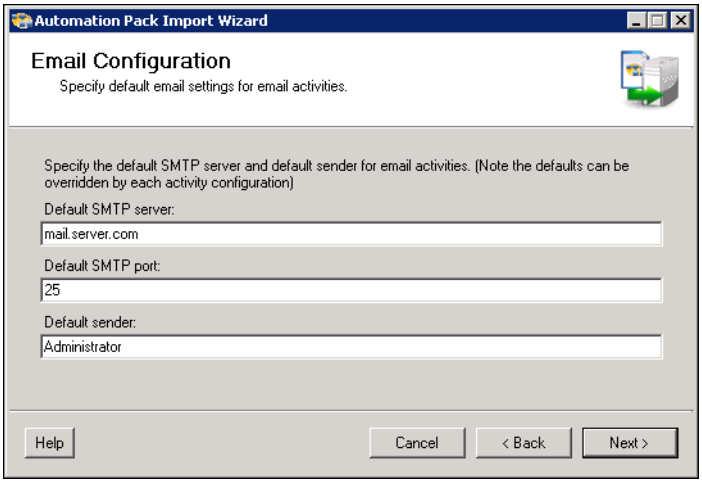
Figure 2-2 Automation Pack Import Wizard—Core—General Information



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.

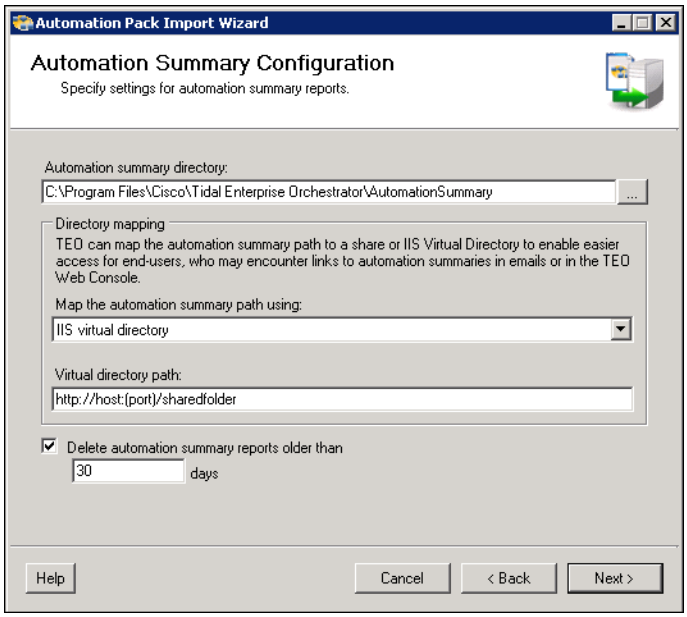
Figure 2-3 Automation Pack Import Wizard—Core—Email Configuration



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.

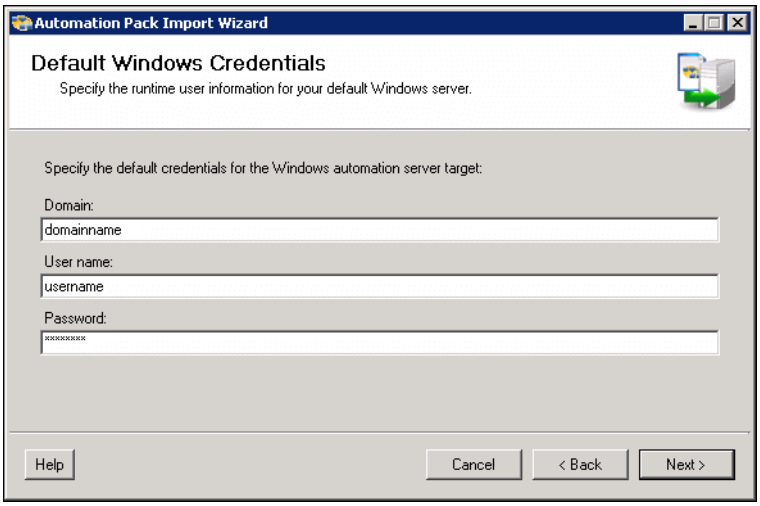
Note You can access the automation summary from Cloud Portal by mapping the automation summary path to an IIS virtual directory. To enable this option, see Step 5.

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: http://host:(port)/sharefolder. 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

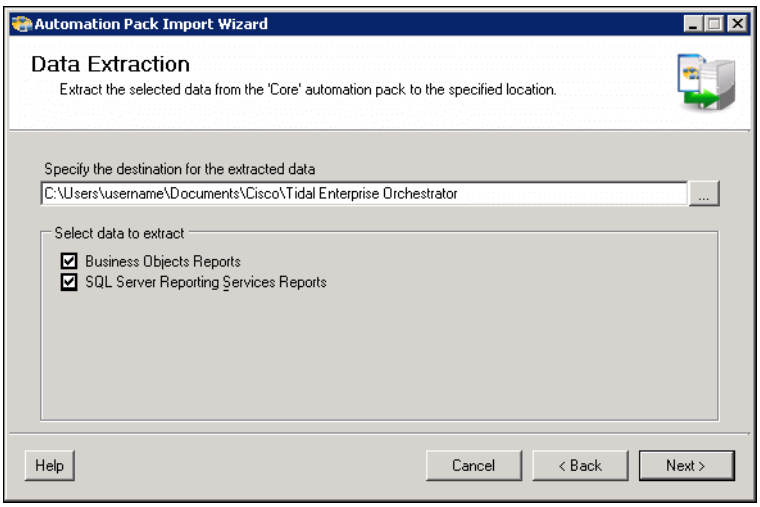


Step 7 On the Default Windows Credentials panel, specify the default credentials for the Windows automation server target.

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.

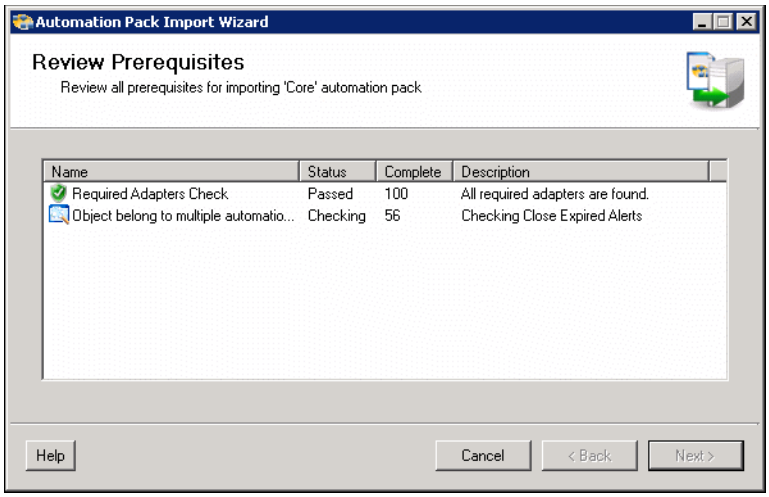
Figure 2-6 Automation Pack Import Wizard—Core—Data Extraction



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.

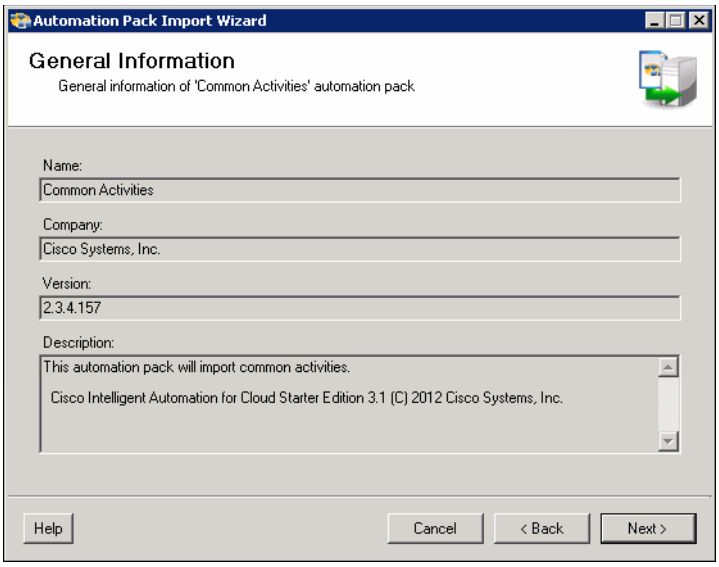
Step 12 Proceed to Import the Common Activities Automation Pack.

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.

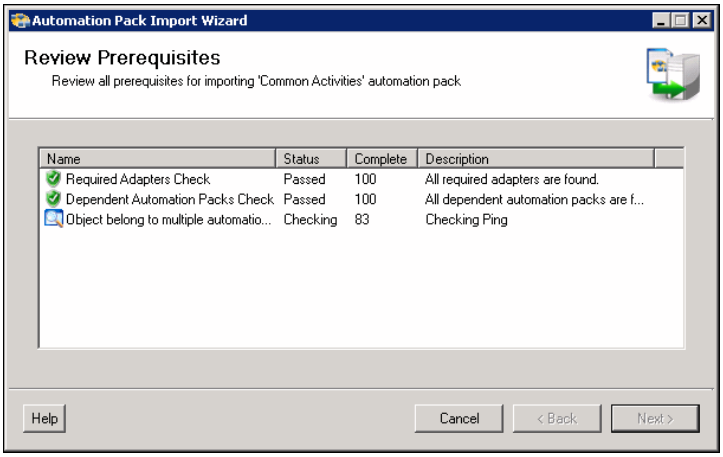
Step 1 On the General Information panel, review the information about the automation pack.

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



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.

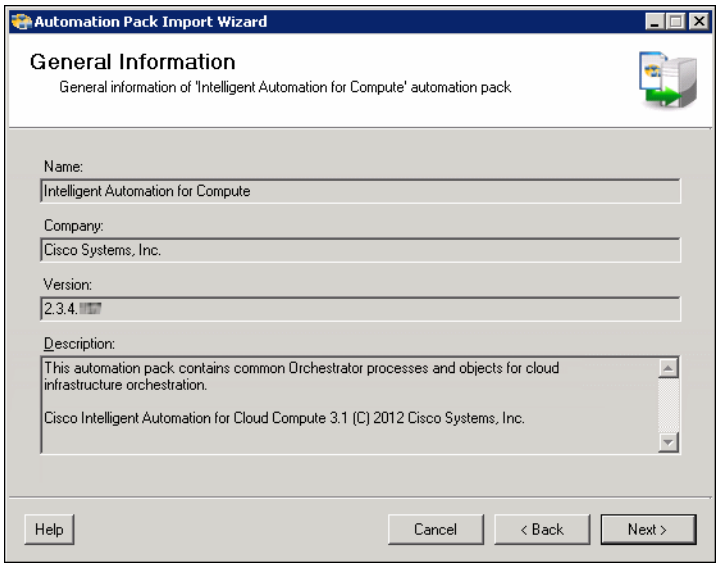
Proceed to Import and Configure the Intelligent Automation for Compute Automation Pack.

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.

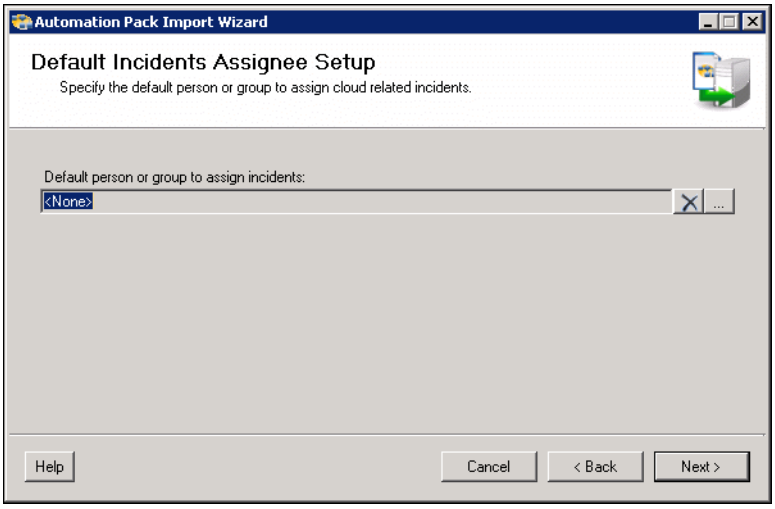
Step 1 On the General Information panel, review the information about the automation pack.

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



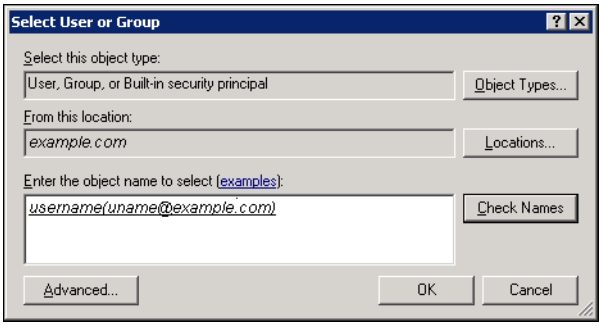
Step 2 Click **Next** to continue.

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.

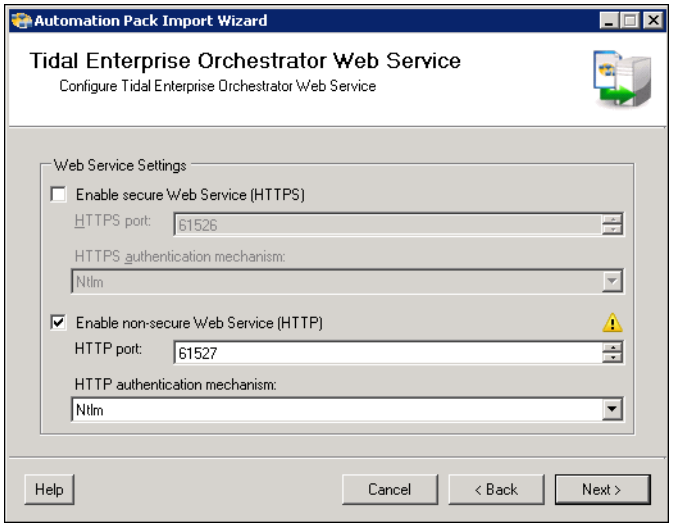
Step 5 In the text box, enter the user name and click **Check Names**.

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

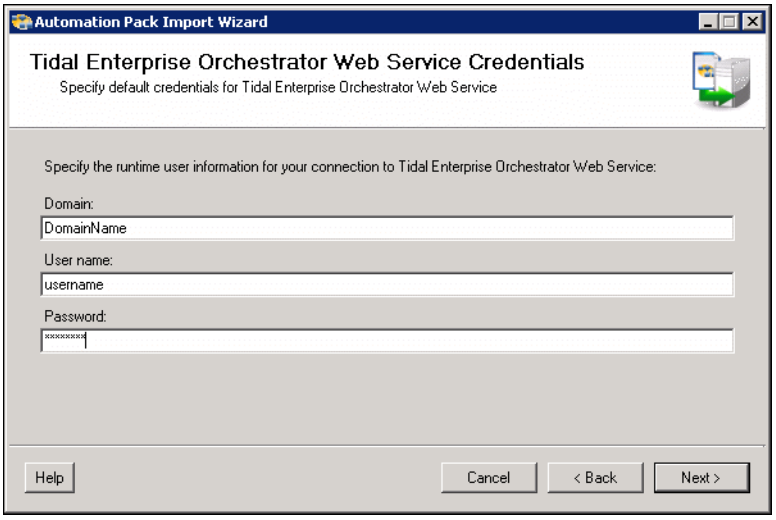


Step 8 On the Tidal Enterprise Orchestrator Web Service panel, specify the following settings:

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: • 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—*Default.* Authentication protocol that is used on networks that include systems running the Windows operating system and on stand-alone systems **Note** The agents in Cloud Portal must also be set to use the same NTLM authentication that you specify here. **Note** In IIS, NTLM is not enabled by default. You must enable NTLM in IIS if you choose this authentication mechanism.

Step 9 Click **Next** to continue.

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

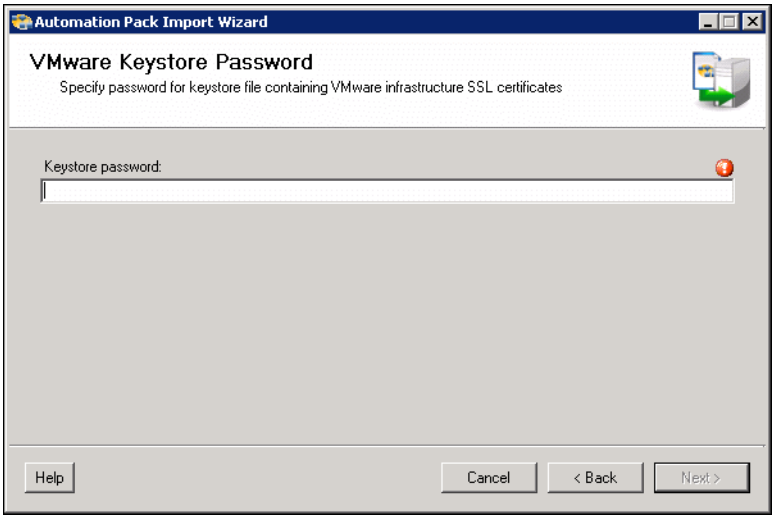


Step 10 On the Default Web Service Credentials panel, specify the credentials for connecting to the Tidal Enterprise Orchestrator web service target:

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.

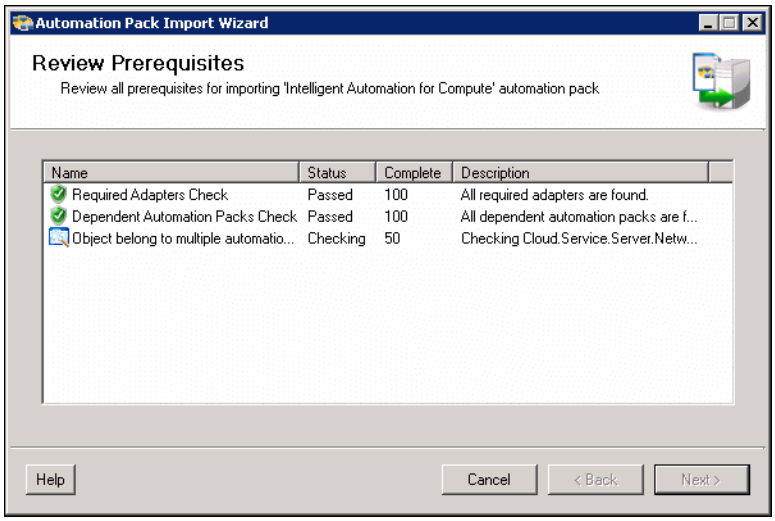
Step 11 Click **Next** to continue.

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.

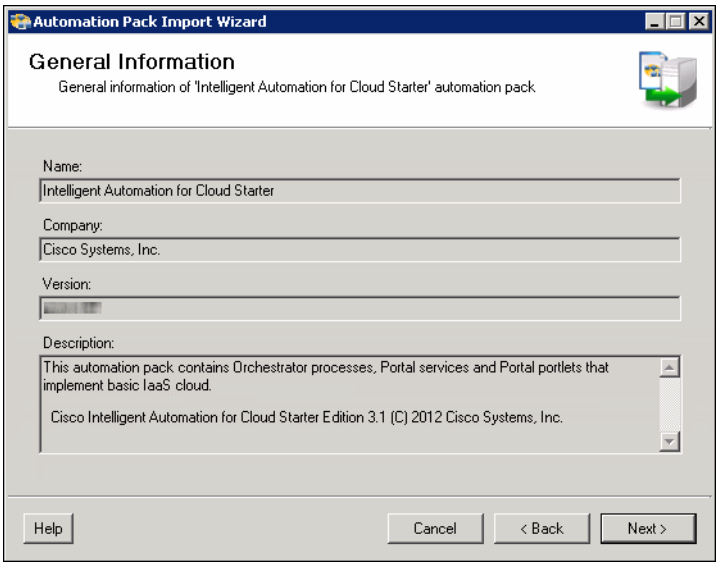
Import and Configure the Intelligent Automation for Cloud Starter Automation Pack

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.

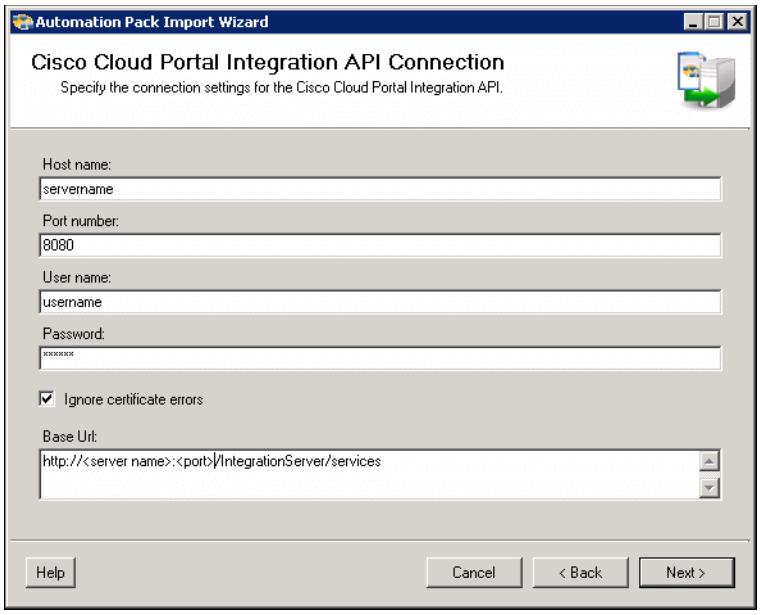
Step 1 On the General Information panel, review the information about the automation pack.

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



Step 2 Click **Next** to continue.

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



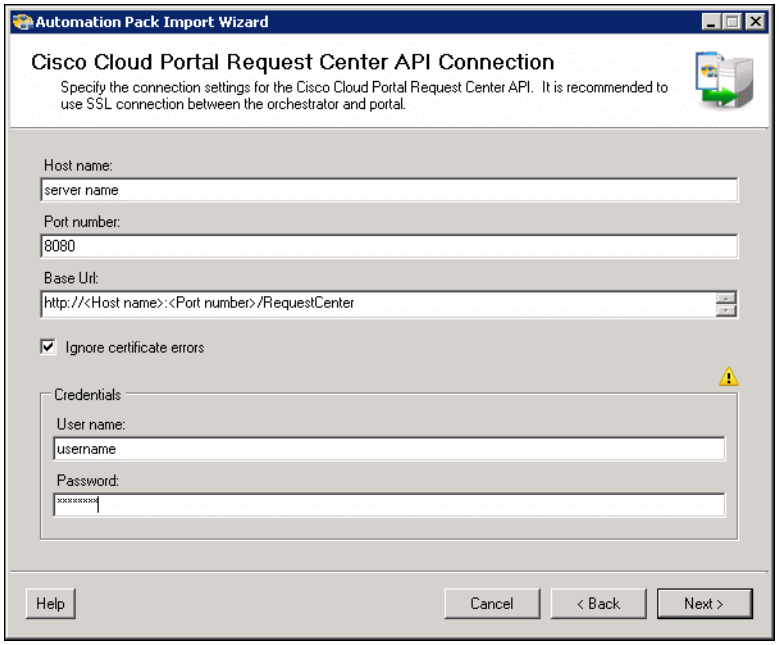
Step 3 On the Cloud Portal Integration API Connection panel, specify for the following information to create a connection to the Cloud Portal:

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	Enter a username and password for the user account that will be used for the connection to Cloud Portal. This user account is referred to as the *nsAPI user account*. Later in the configuration process, you will create the actual account in Cloud Portal using the username and password you set here. **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. **Note** If you change the nsAPI username and password, you must also edit the extended target properties for Cloud.Configuration.CloudPortal.API.Password and Cloud.Configuration.CloudPortal.API.User with the new username. The steps for editing the extended target properties, *see* the *Cisco Intelligent Automation for Cloud User Guide*.
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: http://<Hostname>:<Port>/IntegrationServer/services

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

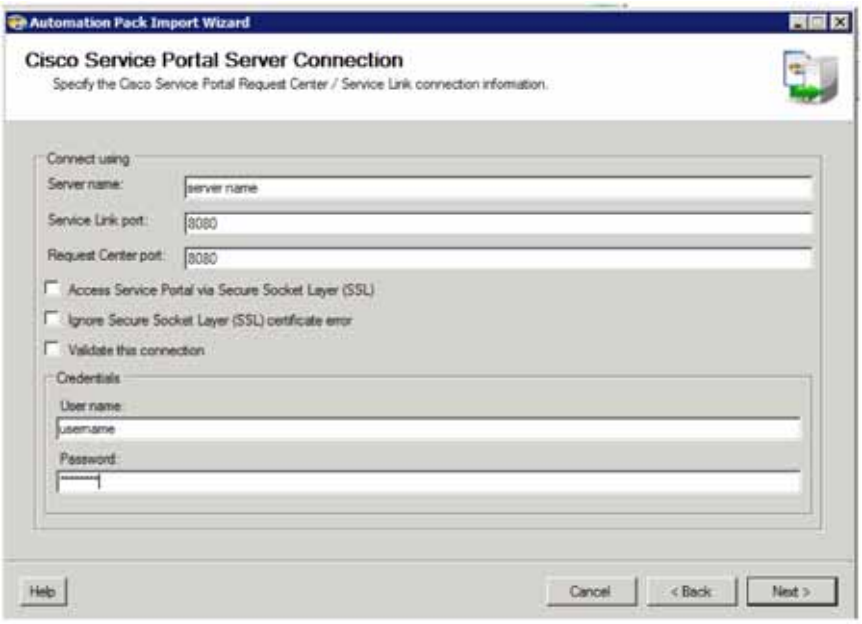


Step 5 On the Cisco Cloud Portal Request Center API Connection panel, specify for the following information for connecting to the Cisco Cloud Portal Request Center API:

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.

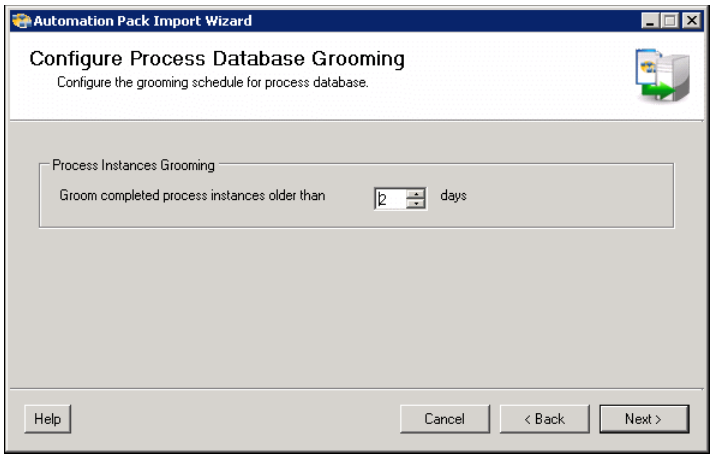
Figure 2-20 Automation Pack Import Wizard—Intelligent Automation for Cloud Starter—Cisco Service Portal Server Connection



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.

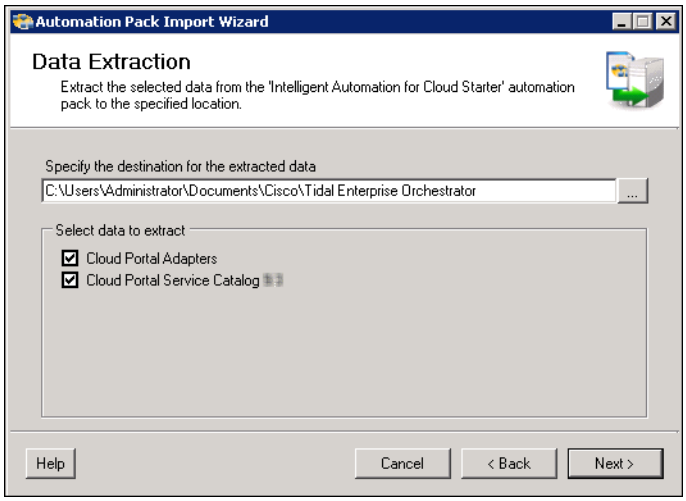
Figure 2-21 Automation Pack Import Wizard—Intelligent Automation for Cloud Starter—Configure Process Database Grooming



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

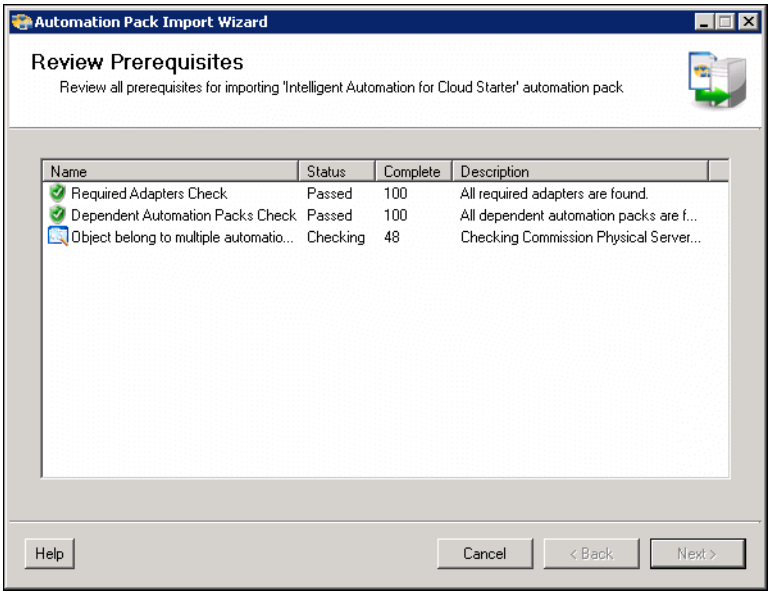


The Data Extraction panel is used to specify the destination where the data is extracted on the Tidal Enterprise Orchestrator server.

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.

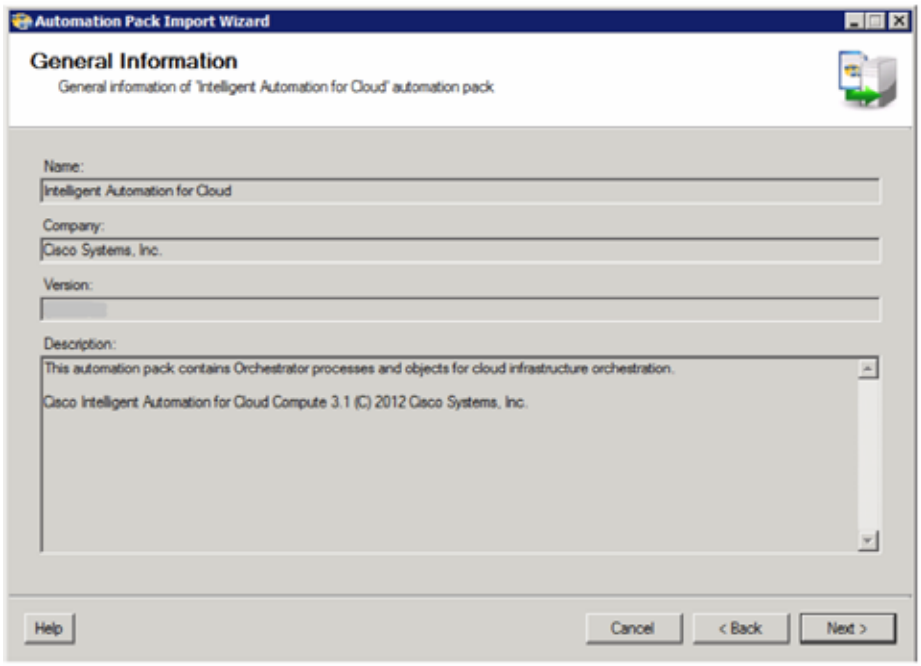
Import and Configure the Intelligent Automation for Cloud Automation Pack

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.

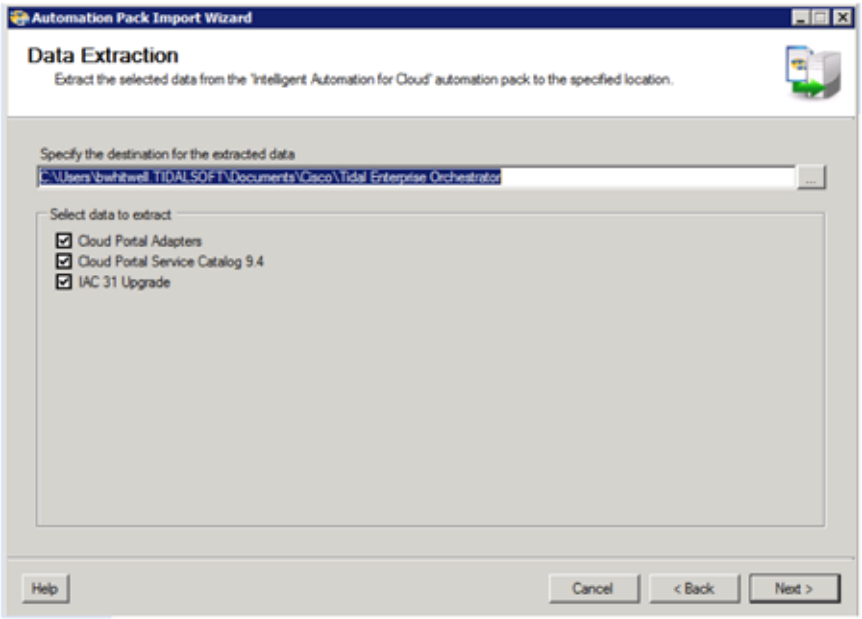
Step 1 On the General Information panel, review the information about the automation pack, then click **Next**.

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



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

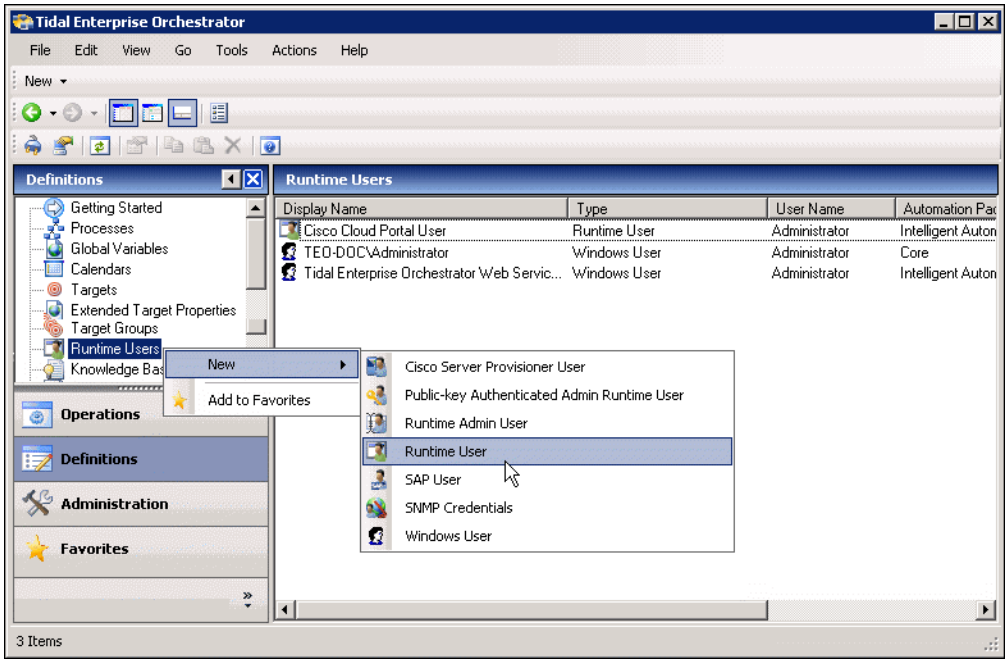
Before you can configure the extended target properties, for Cisco Cloud Portal Integration API, you must first create a Linux target and a default runtime user for the target.

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

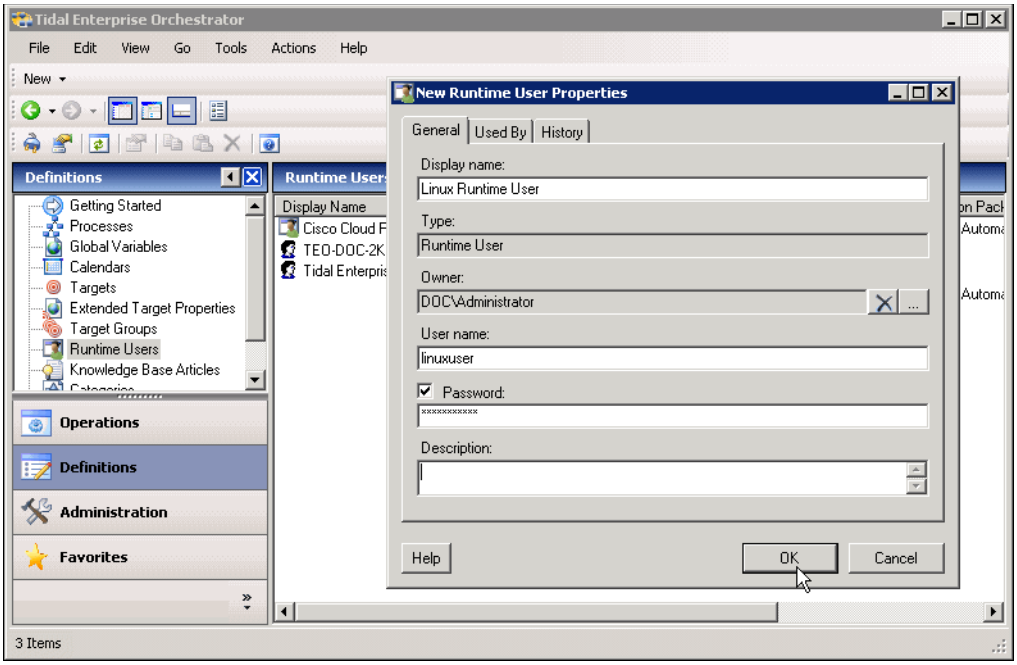


Step 3 In the New Runtime User Properties dialog box, click the **General** tab, and specify the following information:

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	*Optional.* 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.**

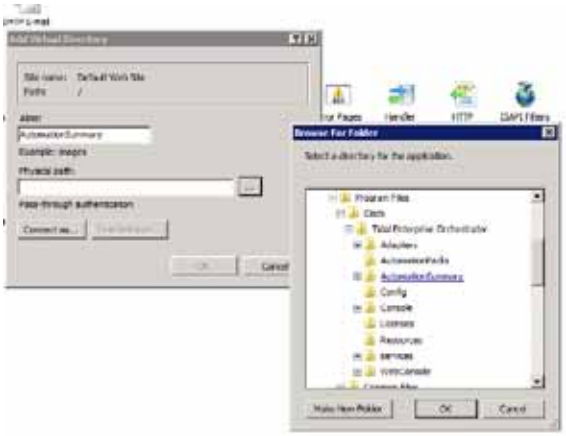
Step 2 Expand *Sites*, right-click on **Default Web Site,** and select **Add Virtual Directory.**

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.

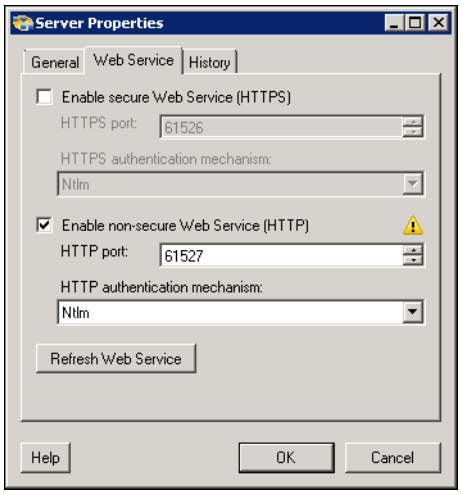
Step 6 Proceed to Refresh Server Web Service.

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.