Using the vCenter Orchestrator Appliance

vCenter Orchestrator 4.2

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.
Using the vCenter Orchestrator Appliance

You can find the most up-to-date technical documentation on the VMware Web site at:
http://www.vmware.com/support/
The VMware Web site also provides the latest product updates.
If you have comments about this documentation, submit your feedback to:
docfeedback@vmware.com

Copyright © 2012 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.
VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com
# Contents

Using the vCenter Orchestrator Appliance 5

Updated Information 7

## 1 Introduction to VMware vCenter Orchestrator 9

- Key Features of the Orchestrator Platform 9
- Orchestrator User Types and Related Responsibilities 10
- Orchestrator Architecture 11
- Orchestrator Plug-Ins 12

## 2 Overview of the Orchestrator Appliance 13

- Download and Deploy the Orchestrator Appliance 14
- Power On the Orchestrator Appliance 14
- Change the Default Root Password 15

## 3 Configuring the Orchestrator Appliance 17

- Log In to the Orchestrator Appliance Web Console 17
- Configure Network Settings for the Orchestrator Appliance 18
- Updating the Orchestrator Appliance 18
  - Check the Orchestrator Appliance Version Status 18
  - Configure the Orchestrator Appliance for Updates 19
  - Install Available Updates Manually 20

## 4 Configuring vCenter Orchestrator 21

- Log In to the Orchestrator Configuration Interface 21
- Import a vCenter Server SSL Certificate and License 22
- Install and Configure the vCenter Server 5.0 Plug-In 23
  - Install the vCenter Server 5.0 Plug-In 23
  - Configure the vCenter Server 5.0 Plug-In 24
- Configuring LDAP Settings 25
  - Generate the LDAP Connection URL 25
  - Import the LDAP Server SSL Certificate 26
  - Specify the Browsing Credentials 27
  - Define the LDAP User and Group Lookup Paths 28
  - Define the LDAP Search Options 29
- Orchestrator Database Setup 29
  - Configure the Database Connection 30
  - Database Connection Parameters 30
- Changing SSL Certificates 31
  - Install a Certificate from a Certificate Authority 31
  - Change the Certificate of the Orchestrator Appliance Management Site 32
Change the SSL Certificate of the Orchestrator Configuration Interface 32

5 The Orchestrator Client and Web Operator 35
  Log In to the Orchestrator Client 35
  Log In to the Orchestrator Web Operator 36

Index 37
Using the vCenter Orchestrator Appliance

Using the vCenter Orchestrator Appliance provides information about deploying and using VMware vCenter Orchestrator™ appliance.

Intended Audience

This information is intended for anyone who wants to use the Orchestrator appliance. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

For more information about Orchestrator, see http://www.vmware.com/support/pubs/orchestrator_pubs.html.
Using the vCenter Orchestrator Appliance is updated with each release of the product or when necessary.

This table provides the update history of Using the vCenter Orchestrator Appliance.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN-000702-01</td>
<td>Updated topics “Change the Default Root Password,” on page 15, “Log In to the Orchestrator Appliance Web Console,” on page 17, and “Log In to the Orchestrator Configuration Interface,” on page 21 for better consistency and more detailed explanation of the change of the default root password.</td>
</tr>
<tr>
<td>EN-000702-00</td>
<td>Initial release.</td>
</tr>
</tbody>
</table>
Introduction to VMware vCenter Orchestrator

VMware vCenter Orchestrator is a development- and process-automation platform that provides a library of extensible workflows to allow you to create and run automated, configurable processes to manage the VMware vSphere infrastructure as well as other VMware and third-party technologies.

Orchestrator exposes every operation in the vCenter Server API, allowing you to integrate all of these operations into your automated processes. Orchestrator also allows you to integrate with other management and administration solutions through its open plug-in architecture.

This chapter includes the following topics:
- “Key Features of the Orchestrator Platform,” on page 9
- “Orchestrator User Types and Related Responsibilities,” on page 10
- “Orchestrator Architecture,” on page 11
- “Orchestrator Plug-Ins,” on page 12

Key Features of the Orchestrator Platform

Orchestrator is composed of three distinct layers: an orchestration platform that provides the common features required for an orchestration tool, a plug-in architecture to integrate control of subsystems, and a library of workflows. Orchestrator is an open platform that can be extended with new plug-ins and libraries, and can be integrated into larger architectures through a SOAP API.

The following list presents the key Orchestrator features.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Persistence</strong></td>
<td>Production grade external databases are used to store relevant information, such as processes, workflow states, and configuration information.</td>
</tr>
<tr>
<td><strong>Central management</strong></td>
<td>Orchestrator provides a central way to manage your processes. The application server-based platform, with full version history, allows you to have scripts and process-related primitives in one place. This way, you can avoid scripts without versioning and proper change control spread on your servers.</td>
</tr>
<tr>
<td><strong>Check-pointing</strong></td>
<td>Every step of a workflow is saved in the database, which allows you to restart the server without losing state and context. This feature is especially useful for long-running processes.</td>
</tr>
<tr>
<td><strong>Versioning</strong></td>
<td>All Orchestrator Platform objects have an associated version history. This feature allows basic change management when distributing processes to different project stages or locations.</td>
</tr>
</tbody>
</table>
**Scripting engine**

The Mozilla Rhino JavaScript engine provides a way to create new building blocks for Orchestrator Platform. The scripting engine is enhanced with basic version control, variable type checking, name space management and exception handling. It can be used in the following building blocks:

- Actions
- Workflows
- Policies

**Workflow engine**

The workflow engine allows you to capture business processes. It uses the following objects to create a step-by-step process automation in workflows:

- Workflows and actions that Orchestrator provides.
- Custom building blocks created by the customer
- Objects that plug-ins add to Orchestrator

Users, other workflows, a schedule, or a policy can start workflows.

**Policy engine**

The policy engine allows monitoring and event generation to react to changing conditions in the Orchestrator server or plugged-in technology. Policies can aggregate events from the platform or any of the plug-ins, which allows you to handle changing conditions on any of the integrated technologies.

**Web 2.0 front end**

The Web 2.0 front end allows you to integrate Orchestrator functions into Web-based interfaces, using Web views. For example, you can create Web views that add buttons to start workflows from a page in your company’s Intranet. It provides a library of user customizable components to access vCO orchestrated objects and uses Ajax technology to dynamically update content without reloading complete pages.

**Security**

Orchestrator provides the following advanced security functions:

- Public Key Infrastructure (PKI) to sign and encrypt content imported and exported between servers
- Digital Rights Management (DRM) to control how exported content might be viewed, edited and redistributed
- Secure Sockets Layer (SSL) encrypted communications between the desktop client and the server and HTTPS access to the Web front end.
- Advanced access rights management to provide control over access to processes and the objects manipulated by these processes.

**Orchestrator User Types and Related Responsibilities**

Orchestrator provides different tools and interfaces based on the specific responsibilities of the two global user roles: Administrators and End Users. Orchestrator developers also have administrative rights and are responsible for creating workflows and additional applications.

**Users with Full Rights**

**Administrators**

This role has full access to all of the Orchestrator platform capabilities. Basic administrative responsibilities include the following items:

- Installing and configuring Orchestrator
- Managing access rights for Orchestrator and applications
- Importing and exporting packages
- Enabling and disabling Web views
- Running workflows and scheduling tasks
- Managing version control of imported elements
- Creating new workflows and plug-ins

**Developers**

This user type has full access to all of the Orchestrator platform capabilities. Developers are granted access to the Orchestrator client interface and have the following responsibilities:

- Creating applications to extend the Orchestrator platform functionality
- Automating processes by customizing existing workflows and creating new workflows and plug-ins
- Customizing Web front ends for automated processes, using Web 2.0 tools.

**Users with Limited Rights**

**End Users**

This role has access to only the Web front end. End users can run and schedule workflows and policies that the administrators or developers make available in a browser by using Web views.

**Orchestrator Architecture**

Orchestrator contains a workflow library and a workflow engine to allow you to create and run workflows that automate orchestration processes. You run workflows on the objects of different technologies that Orchestrator accesses through a series of plug-ins.

Orchestrator provides a standard set of plug-ins, including a plug-in for vCenter Server, to allow you to orchestrate tasks in the different environments that the plug-ins expose.

Orchestrator also presents an open architecture to allow you to plug in external third-party applications to the orchestration platform. You can run workflows on the objects of the plugged-in technologies that you define yourself. Orchestrator connects to a directory services server to manage user accounts, and to a database to store information from the workflows that it runs. You can access Orchestrator, the Orchestrator workflows, and the objects it exposes through the Orchestrator client interface, through a Web browser, or through Web services.
Orchestrator Plug-Ins

Plug-ins allow you to use Orchestrator to access and control external technologies and applications. Exposing an external technology in an Orchestrator plug-in allows you to incorporate objects and functions in workflows that access the objects and functions of that external technology.

The external technologies that you can access by using plug-ins can include virtualization management tools, email systems, databases, directory services, and remote control interfaces.

Orchestrator provides a set of standard plug-ins that you can use to incorporate into workflows such technologies as the VMware vCenter Server API and email capabilities. In addition, you can use the Orchestrator open plug-in architecture to develop plug-ins to access other applications.

The Orchestrator plug-ins that VMware develops are distributed as .vmoapp files, which you can obtain from the VMware Web site at http://www.vmware.com/products/datacenter-virtualization/vcenter-orchestrator/plugins.html. For more information about the Orchestrator plug-ins that VMware develops and distributes, see http://www.vmware.com/support/pubs/vco_plugins_pubs.html.
Overview of the Orchestrator Appliance

The Orchestrator appliance is a preconfigured Linux-based virtual machine optimized for running vCenter Orchestrator.

The Orchestrator appliance packages the following list of software:
- SUSE Linux Enterprise Server 11 Update 1 for VMware, 64-bit edition
- PostgreSQL
- OpenLDAP
- Orchestrator 4.2

The default Orchestrator appliance database configuration is suitable for small- or medium-scale deployment systems. The default OpenLDAP configuration is suitable for experimental and testing purposes only. To use the Orchestrator appliance in a production environment, set up a new database and directory service and configure the Orchestrator server to work with them. For more information about configuring external LDAP and database for production environments, see “Configuring LDAP Settings,” on page 25 and “Orchestrator Database Setup,” on page 29.

The Orchestrator appliance has the following hardware configuration:
- 2 CPUs
- 3GB of memory
- 5GB hard disk

Keep the default memory size or increase it, because the Orchestrator server requires at least 2GB of free memory.

The configuration maximums for the Orchestrator appliance are the same as the maximums for vCenter Orchestrator. For more information, see Configuration Maximums at: http://www.vmware.com/pdf/vsphere5/r50/vsphere-50-configuration-maximums.pdf.

This chapter includes the following topics:
- “Download and Deploy the Orchestrator Appliance,” on page 14
- “Power On the Orchestrator Appliance,” on page 14
- “Change the Default Root Password,” on page 15
Download and Deploy the Orchestrator Appliance

As an alternative to installing vCenter Orchestrator on a Windows computer, you can download and deploy the Orchestrator appliance.

Prerequisites

Verify that your computing environment meets the following conditions:

- vCenter Server is installed and running.
- vSphere Client is installed.
- The host on which you are deploying the appliance has at least 5GB of free disk space.

In case that your system is isolated and without Internet access, you must download the .vmdk and .ovf files for the appliance from the download page on the VMware Web site, and save the files in the same folder.

Procedure

1. Log in to the vSphere Client as an administrator.
2. In the vSphere Client, select File > Deploy OVF Template.
3. Enter the path or the URL to the .ovf file and click Next.
4. Review the OVF details and click Next.
5. Accept the terms in the license agreement and click Next.
6. Specify a name and location for the deployed appliance and select a host or cluster on which to run the appliance.
7. Select a format in which to store the appliance's virtual disk.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thick provisioned format</td>
<td>Select to commit to using the maximum 5GB of disk space at deployment. VMware recommends that you select to deploy the OVF with thick provisioning.</td>
</tr>
<tr>
<td>Thin provisioned format</td>
<td>Select to deploy the OVF with thin provisioning, if you do not want to commit to using the maximum 5GB of disk space at deployment.</td>
</tr>
</tbody>
</table>

8. (Optional) Specify the network settings and IP address allocation, and click Next.

   By default the Orchestrator appliance uses DHCP. You can also change this setting manually and assign a fixed IP address from the appliance Web console.

9. Review the properties and the Ready to Complete Page and optionally select to power on the appliance after deployment.
10. Click Finish.

The Orchestrator appliance is successfully deployed.

Power On the Orchestrator Appliance

To use the Orchestrator appliance you must first power it on and log in to get the virtual appliance IP address.

Procedure

1. Log in to the vSphere Client as an administrator.
2. Right-click the Orchestrator appliance and select Power > Power On.
3 Click the Summary tab to view the Orchestrator appliance IP address.

**What to do next**

Log in to the Orchestrator appliance Web interface and change the default root password.

### Change the Default Root Password

For security reasons, you must change the root password the first time you attempt to open the Orchestrator configuration interface or the appliance configuration.

**Prerequisites**

- Log in to the vSphere Client as an administrator.
- Download and deploy the Orchestrator appliance.
- Ensure that the appliance is up and running.

**Procedure**

1. Select the appliance in the vSphere Client inventory and click the Summary tab.
   
   You can see the IP address of the Orchestrator appliance.

2. In a Web browser, navigate to the IP address that your Orchestrator appliance virtual machine provides.
   
   http://orchestrator_appliance_ip

3. Click Appliance Configuration.
   
   A page where you can change the default password for the root user of the appliance is loaded.

4. Respond to the prompts to type and retype your new password.

5. Click Change password.

You successfully changed the password of the root Linux user of the Orchestrator appliance. You are redirected to the Orchestrator appliance Web console.
The Orchestrator appliance is a preconfigured Linux-based virtual appliance. Before you use it, you might want to edit some of the configuration settings of the appliance.

The Orchestrator appliance is built with VMware Studio. For more information about virtual appliances created with VMware Studio, see the VMware Studio documentation at http://www.vmware.com/support/developer/studio/index.html.

This chapter includes the following topics:

- “Log In to the Orchestrator Appliance Web Console,” on page 17
- “Configure Network Settings for the Orchestrator Appliance,” on page 18
- “Updating the Orchestrator Appliance,” on page 18

Log In to the Orchestrator Appliance Web Console

Log in to the Orchestrator appliance Web console to access the appliance configuration settings.

Prerequisites

- Download and deploy the Orchestrator appliance.
- Ensure that the appliance is up and running.
- Ensure that you change the root password of the appliance Linux user. Otherwise, the first time when you try to log in to the appliance Web console, you will be prompted to change the password. For more information, see “Change the Default Root Password,” on page 15.

Procedure

1. In a Web browser, navigate to the IP address that your Orchestrator appliance virtual machine provides.

   http://orchestrator_appliance_ip

2. Click Appliance Configuration to go to the appliance Web console.

3. Type the Orchestrator appliance user name and password, and click Login.

You can view the system settings of the Orchestrator appliance, such as vendor, appliance name, and version.

What to do next

Edit the network or update settings of the appliance.
Configure Network Settings for the Orchestrator Appliance

Configure network settings for the Orchestrator appliance to assign a static IP and define the proxy settings.

**Prerequisites**
- Download and deploy the Orchestrator appliance.
- Ensure that the appliance is up and running.

**Procedure**
1. Log in to the Orchestrator appliance Web console.
2. On the Network tab, click **Address**.
3. Select the method by which the appliance obtains IP address settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>Obtains IP settings from a DHCP server. This is the default setting.</td>
</tr>
<tr>
<td>Static</td>
<td>Uses static IP settings. Specify the IP address, netmask, and gateway.</td>
</tr>
</tbody>
</table>
4. (Optional) Type the necessary network configuration information.
5. Click **Save Settings**.
6. (Optional) Use a proxy server for the Orchestrator appliance.
   a. On the Network tab, click **Proxy**.
   b. Select **Use a proxy server** to use a proxy server for the Orchestrator appliance.
   c. Specify a proxy server and a proxy port.
   d. Type a proxy user name and proxy password if your proxy server requires them.
   e. Click **Save Settings**.

**Updating the Orchestrator Appliance**

You can update the deployed Orchestrator appliance with packages that VMware publishes. You can perform updates over the external Web, on your local area network, or from a CD-ROM.

To conserve network bandwidth, virtual appliance updates are applied only to packages that have changed. Updates can apply to the operating system, applications in the virtual appliance, VMware Tools, or the VMware Appliance Management Infrastructure (VAMI).

If you have installed VMware vSphere® Update Manager you can use it to update the Orchestrator appliance automatically. For more information about upgrading virtual appliances with vSphere Update Manager, see the Update Manager documentation at [http://www.vmware.com/support/pubs/vum_pubs.html](http://www.vmware.com/support/pubs/vum_pubs.html).

**Check the Orchestrator Appliance Version Status**

You might want to see and check the Orchestrator appliance version status before you configure the appliance for updates.

**Prerequisites**
- Download and deploy the Orchestrator appliance.
- Ensure that the appliance is up and running.
Procedure

1. Log in to the Orchestrator appliance Web console.
2. On the **Update** tab, click **Status**.

You see the update status of the Orchestrator appliance.

**What to do next**
Configure the Orchestrator appliance for updates.

**Configure the Orchestrator Appliance for Updates**

You can update a deployed Orchestrator appliance with packages that VMware publishes. You can perform updates over the external Web, on your local area network, or from a CD-ROM.

**Prerequisites**
- Download and deploy the Orchestrator appliance.
- Ensure that the appliance is up and running.

**Procedure**

1. Log in to the Orchestrator appliance Web console.
2. On the **Update** tab, click **Settings**.
3. Set an update policy for the virtual appliance.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No automatic updates</strong></td>
<td>The virtual appliance does not check for and install updates.</td>
</tr>
<tr>
<td><strong>Automatic check for updates</strong></td>
<td>The virtual appliance checks for updates at the scheduled time. If an update is available, it appears on the Update Status page.</td>
</tr>
<tr>
<td><strong>Automatic check and install updates</strong></td>
<td>The virtual appliance checks for updates at the scheduled time. If an update is available, the virtual appliance installs it.</td>
</tr>
</tbody>
</table>

If you select either **Automatic check for updates** or **Automatic check and install updates**, you can configure the scheduling. By default, the check occurs daily at 03:00 local time, as determined by your time zone settings.

4. Set up the update repository location.

The default is the URL that VMware configured. You might need to change the update source or location if you are updating inside a restricted local area network.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Use CD-ROM Updates</strong></td>
<td>Insert the update CD-ROM in a drive that the virtual appliance can read. The update agent scans the CD drives to find the first update CD-ROM.</td>
</tr>
<tr>
<td><strong>Use Specified Repository</strong></td>
<td>Type the URL of the update repository for your appliance to check. If the URL requires authentication, provide a valid user name and password.</td>
</tr>
</tbody>
</table>

5. Click **Save Settings**.
Install Available Updates Manually

When new updates for the Orchestrator appliance become available, you might want to install them to keep your appliance up-to-date.

Prerequisites

- Download and deploy the Orchestrator appliance.
- Ensure that the appliance is up and running.

Procedure

1. Log in to the Orchestrator appliance Web console.
2. On the Update tab, click Status.
3. Under the Actions section, click Check Updates.
   - The virtual appliance connects to the update repository and checks for available updates. Updates appear in the Available Updates pane.
4. To install an update, click Install Updates.
Although the Orchestrator appliance is a preconfigured Linux-based virtual machine, you might want to change the Orchestrator settings. If you want to use the Orchestrator appliance in a medium or large-scale environment, also change the LDAP and database settings.

The Orchestrator appliance contains a preconfigured PostgreSQL database and OpenLDAP server. The PostgreSQL database and OpenLDAP server are accessible only locally from the virtual appliance Linux console.

While PostgreSQL is suitable for small- to medium-scale production environments, you should change OpenLDAP with an external supported directory service. For more information about setting up an external directory service, see “Configuring LDAP Settings,” on page 25.

Preconfigured software | User group (if any) and user | Password
--- | --- | ---
PostgreSQL | User: vmware | vmware
OpenLDAP | User group: vcoadmins | vcoadmin
User: vcoadmin
By default the vcoadmin user is set up as an Orchestrator administrator.
OpenLDAP | User group: vcousers | vcouser
User: vcouser

For more information about configuring Orchestrator, see Installing and Configuring VMware vCenter Orchestrator.

This chapter includes the following topics:

- “Log In to the Orchestrator Configuration Interface,” on page 21
- “Import a vCenter Server SSL Certificate and License,” on page 22
- “Install and Configure the vCenter Server 5.0 Plug-In,” on page 23
- “Configuring LDAP Settings,” on page 25
- “Orchestrator Database Setup,” on page 29
- “Changing SSL Certificates,” on page 31

Log In to the Orchestrator Configuration Interface

To edit the default configuration settings of the Orchestrator server and to assign a server certificate, you must log in to the Orchestrator configuration interface.

Prerequisites

- Download and deploy the Orchestrator appliance.
Ensure that the appliance is up and running.

Ensure that you change the root password of the appliance Linux user. Otherwise, the first time when you try to log in to the Orchestrator configuration interface, you will be prompted to change the password. For more information, see “Change the Default Root Password,” on page 15.

**Procedure**

1. In a Web browser, navigate to the IP address that your Orchestrator appliance virtual machine provides.
   
   http://orchestrator_appliance_ip

2. Click Orchestrator Configuration.

3. Log in with the default credentials.
   - User name: vmware
     You cannot change the default user name.
   - Password: vmware
     When you log in to the Orchestrator configuration interface with the default password, you see the Welcome page prompting you to change the default password of the Orchestrator configuration interface.

4. Type and confirm your new password.

5. Click Apply changes.

---

**Import a vCenter Server SSL Certificate and License**

The Orchestrator appliance is distributed with a built-in evaluation license that expires 90 days after you power on the appliance for the first time. To continue using the Orchestrator appliance after the trial period, you must import a vCenter Server license.

The Orchestrator configuration interface uses a secure connection to communicate with vCenter Server. You can import the required SSL certificate from a URL or file.

For more information about vCenter Server license and access rights to the Orchestrator server, see *Installing and Configuring VMware vCenter Orchestrator*.

The user you select must be a valid user with administrative privileges on your vCenter Server system, preferably at the top of the vSphere tree structure.

**Procedure**

1. Log in to the Orchestrator configuration interface as vmware.

2. Click Network.

3. In the right pane, click the SSL Certificate tab.

4. Load the vCenter Server SSL certificate in Orchestrator from a URL address or file.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import from URL</td>
<td>Specify the URL of the vCenter Server:</td>
</tr>
<tr>
<td></td>
<td>https://your_vcenter_server_IP_address</td>
</tr>
<tr>
<td>Import from file</td>
<td>Obtain the vCenter Server certificate file. The file is usually available at the following locations:</td>
</tr>
<tr>
<td></td>
<td>C:\Documents and Settings\AllUsers\ApplicationData\VMware\VMwareVirtualCenter\SSL\rui.crt</td>
</tr>
<tr>
<td></td>
<td>/etc/vmware/ssl/rui.crt</td>
</tr>
</tbody>
</table>
5 Click **Import**.
A message confirming that the import is successful appears.

6 In the Orchestrator configuration interface, click **Licenses**.

7 Click the **vCenter Server License** tab, and click **Use vCenter Server license**.

8 Specify the details about the vCenter Server host on which Orchestrator must verify the license key.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host</strong></td>
<td>Type the IP address or the DNS name of the vCenter Server host.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Leave the default value (443).</td>
</tr>
<tr>
<td><strong>Secure channel</strong></td>
<td>(Optional) Select to establish a secure connection to the vCenter Server host.</td>
</tr>
<tr>
<td><strong>Path</strong></td>
<td>Use the default value, <code>/sdk</code>.</td>
</tr>
<tr>
<td><strong>User name</strong></td>
<td>Type the credentials that Orchestrator must use to establish the connection to vCenter Server.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Type the credentials that Orchestrator must use to establish the connection to vCenter Server.</td>
</tr>
</tbody>
</table>

9 Click **Apply changes**.

10 Restart the Orchestrator server.

### Install and Configure the vCenter Server 5.0 Plug-In

Orchestrator uses the vCenter Web Service API to control vCenter Server. You can install the vCenter Server 5.0 plug-in and then set the parameters to enable Orchestrator to connect to your vCenter Server instances.

#### Procedure

1 **Install the vCenter Server 5.0 Plug-In** on page 23

Orchestrator uses the vCenter Web Service API to control vCenter Server. You can install the vCenter Server 5.0 plug-in and then set the parameters to enable Orchestrator to connect to your vCenter Server instances.

2 **Configure the vCenter Server 5.0 Plug-In** on page 24

Orchestrator uses the vCenter Web Service API to control vCenter Server. You can set the parameters to enable Orchestrator to connect to your vCenter Server instances.

### Install the vCenter Server 5.0 Plug-In

Orchestrator uses the vCenter Web Service API to control vCenter Server. You can install the vCenter Server 5.0 plug-in and then set the parameters to enable Orchestrator to connect to your vCenter Server instances.

#### Procedure

1 Log in to the Orchestrator configuration interface as vmware.

2 Click the **Plug-ins** tab.

3 In the list of plug-ins on the left, select **vCenter Server**, and click **Apply changes**.

4 Click the **Startup options** tab.

5 Click **Restart the vCO configuration server**.

The vCenter Server 5.0 plug-in tab becomes active and you can configure the connection between vCenter Orchestrator and vCenter Server instances.
Configure the vCenter Server 5.0 Plug-In

Orchestrator uses the vCenter Web Service API to control vCenter Server. You can set the parameters to enable Orchestrator to connect to your vCenter Server instances.

**Prerequisites**

Import the SSL certificates for each vCenter Server instance you define. See *Installing and Configuring VMware vCenter Orchestrator*.

**Procedure**

1. Log in to the Orchestrator configuration interface as vmware.
2. Click **vCenter Server 5.0**.
3. Click **New vCenter Server Host**.
4. From the **Available** drop-down menu, select **Enabled**.
5. In the **Host** text box, type the IP address or the DNS name of the vCenter Server host.
6. In the **Port** text box, retain the default value, 443.
7. (Optional) Select the **Secure channel** check box to establish a secure connection to your vCenter Server host.
8. In the **Path** text box, retain the default value, /sdk.
   This value is the location of the SDK that you use to connect to your vCenter Server instance.
9. In the **User name** and **Password** text boxes, type the credentials for Orchestrator to use to establish the connection to the vCenter Server host.
   The user that you select must be a valid user with administrative privileges on your vCenter Server, preferably at the top of the vCenter Server tree structure. Orchestrator uses these credentials to monitor the vCenter Web service, typically to operate Orchestrator system workflows. All other requests inherit the credentials of the user who triggers an action.
10. Select the method you use to manage user access on the vCenter Server host.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share a unique session</td>
<td>Allows Orchestrator to create only one connection to vCenter Server. Type the credentials of a user who is a vCenter Server administrator.</td>
</tr>
<tr>
<td><strong>Session per user</strong></td>
<td><strong>CAUTION</strong> Each user who logs in to Orchestrator creates a new session to vCenter Server. This might rapidly use CPU, memory, and bandwidth. Select this option if your vCenter Server is in an Active Directory domain. Make sure that the user has the necessary permissions to perform the required operations.</td>
</tr>
</tbody>
</table>

11. Click **Apply changes**.
   The URL to the newly configured vCenter Server host is added to the list of defined hosts.
12. Repeat Step 3 through Step 11 for each vCenter Server instance.
Configuring LDAP Settings

The Orchestrator appliance contains a preconfigured OpenLDAP server that is suitable for experimental use in small- and medium-scale environments. To use the Orchestrator appliance in a large-scale environment for production purposes, set up a new directory service server and configure Orchestrator to work with it.


Connect your system to the LDAP server that is physically closest to your Orchestrator server, and avoid connections to remote LDAP servers. Long response times for LDAP queries can lead to slower performance of the whole system.

To improve the performance of the LDAP queries, keep the user and group lookup base as small as possible. Limit the users to targeted groups that need access, rather than to whole organizations with many users who do not need access. Depending on the combination of database and directory service you choose, the resources you need can vary. For recommendations, see the documentation for your LDAP server.

Generate the LDAP Connection URL

The LDAP service provider uses a URL to configure the connection to the directory server. To generate the LDAP connection URL, you must specify the LDAP host, port, and root.

The supported directory service types are Active Directory, eDirectory, and Sun Java System Directory Server.

Procedure

1. Log in to the Orchestrator configuration interface as vmware.
2. Click LDAP.
3. From the LDAP client drop-down menu, select the directory server type that you are using as the LDAP server.

   **Note:** If you change the LDAP server or type after you set permissions on Orchestrator objects (such as access rights on workflows or actions), you must reset these permissions.

   If you change the LDAP settings after configuring custom applications that capture and store user information, the LDAP authentication records created in the database become invalid when used against the new LDAP database.

4. In the Primary LDAP host text box, type the IP address or the DNS name of the host on which your primary LDAP service runs.

   This is the first host on which the Orchestrator configuration interface verifies user credentials.

5. (Optional) In the Secondary LDAP host text box, type the IP address or the DNS name of the host on which your secondary LDAP service runs.

   If the primary LDAP host becomes unavailable, Orchestrator verifies user credentials on the secondary host.

6. In the Port text box, type the value for the lookup port of your LDAP server.

   **Note:** Orchestrator supports the Active Directory hierarchical domains structure. If your domain controller is configured to use Global Catalog, you must use port 3268. You cannot use the default port 389 to connect to the Global Catalog server.
7 In the **Root** text box, type the root element of your LDAP service.

If your domain name is *company.org*, your root LDAP is `dc=company,dc=org`.

This is the node used for browsing your service directory after typing the appropriate credentials. For large service directories, specifying a node in the tree narrows the search and improves performance. For example, rather than searching in the entire directory, you can specify `ou=employees,dc=company,dc=org`.

This displays all the users in the Employees group.

8 (Optional) Select **Use SSL** to activate encrypted certification for the connection between Orchestrator and LDAP.

If your LDAP uses SSL, you must first import the SSL certificate and restart the Orchestrator Configuration service. See “Import the LDAP Server SSL Certificate,” on page 26.

9 (Optional) Select **Use Global Catalog** to allow LDAP referrals when the LDAP client is Active Directory.

The LDAP server lookup port number changes to 3268. Orchestrator follows the LDAP referrals to find users and groups in a subdomain that is part of the Active Directory tree to which Orchestrator is connected. You can add permissions on any groups that can be accessed from your Global Catalog.

**Example: Values and Resulting LDAP Connection URL Addresses**

Examples of the values that you enter in the required fields and the resulting LDAP connection URL.

- **LDAP host:** *DomainController*
- **Port:** 389
- **Root:** `ou=employees,dc=company,dc=org`

Connection URL: `ldap://DomainController:389/ou=employees,dc=company,dc=org`

- **LDAP host using Global Catalog:** *10.23.90.130*
- **Port:** 3268
- **Root:** `dc=company,dc=org`

Connection URL: `ldap://10.23.90.130:3268/dc=company,dc=org`

**What to do next**

Assign credentials to Orchestrator to ensure its access to the LDAP server. See “Specify the Browsing Credentials,” on page 27.

**Import the LDAP Server SSL Certificate**

If your LDAP server uses SSL, you can import the SSL certificate file to the Orchestrator configuration interface and activate secure connection between Orchestrator and LDAP.

For instructions about configuring your LDAP server for SSL access, see third-party documentation.

**Prerequisites**

- Verify that SSL access is enabled on the LDAP server.
- If you are using LDAPS, Windows 2003 or 2008, and AD, verify that the **LDAP Server Signing Requirements** group policy is disabled on the LDAP server.
- Obtain a self-signed server certificate or a certificate that is signed by a Certificate Authority.

**Procedure**

1 Log in to the Orchestrator configuration interface as vmware.
2 Click **Network**.

3 In the right pane, click the **SSL Certificate** tab.

4 Browse to select a certificate file to import.

5 Click **Import**.
   
   A message confirming that the import is successful appears.

6 Click **Startup Options**.

7 Click **Restart the vCO configuration server** to restart the Orchestrator Configuration service after adding a new SSL certificate.

The imported certificate appears in the Imported SSL certificates list. You activated secure connection between Orchestrator and your LDAP server.

**What to do next**

You must enable SSL on the **LDAP** tab in the Orchestrator configuration interface.

**Specify the Browsing Credentials**

Orchestrator must read your LDAP structure to inherit its properties. You can specify the credentials that Orchestrator uses to connect to an LDAP server.

**Prerequisites**

Ensure that you have a working LDAP service in your infrastructure and have generated the LDAP connection URL.

**Procedure**

1 Log in to the Orchestrator configuration interface as *vmware*.

2 Click **LDAP**.

3 Specify the primary and secondary LDAP hosts, the lookup port of the LDAP server, and the root element.

4 Type a valid user name (LDAP string) in the **User name** text box for a user who has browsing permissions on your LDAP server.

   The possible formats in which you can specify the user name in Active Directory are as follows:
   
   - Bare user name format, for example *user*.
   - Distinguished name format: *cn=user,ou=employees,dc=company,dc=org*.
     
     Use this format with Sun and eDirectory. Do not use spaces between the comma and the next identifier.
   - Principal name format: *user@company.org*.
   - NetBEUI format: *COMPANY\user*.

5 In the **Password** text box, type the password for the user name you entered in **Step 4**.

   Orchestrator uses the credentials to connect to the LDAP server.

**What to do next**

Define the LDAP containers for Orchestrator to look up users and groups.
Define the LDAP User and Group Lookup Paths

You can define the users and groups lookup information.

Two global roles are identified in Orchestrator: Developers and Administrators. The users in the Developers role have editing privileges on all elements. The users in the Administrators role have unrestricted privileges. Administrators can manage permissions, or discharge administration duties on a selected set of elements to any other group or user. These two groups must be contained in the Group lookup base.

Prerequisites

You must have a working LDAP service on your infrastructure.

Procedure

1. Log in to the Orchestrator configuration interface as vmware.
2. Click LDAP.
3. Specify the primary and secondary LDAP hosts, the lookup port of the LDAP server, the root element, and the browsing credentials.
4. Define the User lookup base.
   - This is the LDAP container (the top-level domain name or organizational unit) where Orchestrator searches for potential users.
     a. Click Search and type the top-level domain name or organizational unit.
        Searching for company returns dc=company,dc=org and other common names containing the search term. If you type dc=company,dc=org as a search term, no results are found.
     b. Click the LDAP connection string for the discovered branch to insert it in the User lookup base text box.
        If no matches are found, check your LDAP connection string in the main LDAP page.
        Note: You can connect to the Global Catalog Server through port 3268. It issues LDAP referrals that Orchestrator follows to find the account or group in a subdomain.
5. Define the Group lookup base.
   - This is the LDAP container where Orchestrator looks up groups.
     a. Click Search and type the top-level domain name or organizational unit.
     b. Click the LDAP string for the discovered branch to insert it in the Group lookup base text box.
6. Define the vCO Admin group.
   - This must be an LDAP group (like Domain Users) to which you grant administrative privileges for Orchestrator.
     a. Click Search and type the top-level group name.
     b. Click the LDAP string for the discovered branch to insert it in the vCO Admin group text box.

Important: In eDirectory installations, only the eDirectory administrator can see users or user groups that have administration rights. If you are using an eDirectory LDAP server, and you log in to Orchestrator as a member of the vCO Admin group but you are not the eDirectory administrator, you can create users or user groups with administration rights, but you cannot see those users. This problem does not apply to other LDAP servers.
7 Click the **Test Login** tab and type credentials for a user to test whether they can access the Orchestrator smart client.

After a successful login, the system checks if the user is part of the Orchestrator Administrator group.

**What to do next**

Define the LDAP search options and apply your changes.

### Define the LDAP Search Options

You can customize the LDAP search queries and make searching in LDAP more effective.

**Procedure**

1. Log in to the Orchestrator configuration interface as vmware.
2. Click **LDAP**.
3. In the **Request timeout** text box, type a value in milliseconds.
   
   This value determines the period during which the Orchestrator server sends a query to the service directory, the directory searches, and sends a reply. If the timeout period elapses, modify this value to check whether the timeout occurs in the Orchestrator server.
4. (Optional) For all links to be followed before the search operation is performed, select the **Dereference links** check box.
   
   Sun Java System Directory Server does not support reference links. If you are using un Java System Directory Server, you must select the **Dereference links** check box.
5. (Optional) Select the **Filter attributes** check box to filter the attributes that the search returns.
   
   Selecting this check box makes searching in LDAP faster. You might need to use some extra LDAP attributes for automation later.
6. (Optional) Select the **Ignore referrals** check box to disable referral handling.
   
   When you select the check box, the system does not display any referrals.
7. In the **Host reachable timeout** text box, type a value in milliseconds.
   
   This value determines the timeout period for the test that is checking the status of the destination host.
8. Click **Apply changes**.

On the **LDAP** tab, the red triangle changes to a green circle to indicate that the component is now configured correctly.

### Orchestrator Database Setup

The Orchestrator appliance contains a preconfigured and prepopulated PostgreSQL database that is suitable for small- and medium-scale environments. To use the Orchestrator appliance in a production environment, set up a new database and configure the Orchestrator server to connect to that database.

Orchestrator server supports Oracle and Microsoft SQL Server databases.

The common workflow for setting up the Orchestrator database involves the following tasks:

1. Create a new database. For more information about creating a new database, see the documentation of your Microsoft or Oracle database provider.
2. Enable the database for remote connection.
3. Configure the database connection parameters. For more information, see “Configure the Database Connection,” on page 30.
The way in which your database is set up can affect Orchestrator performance.

The size of the Orchestrator database varies depending on the setup and how workflow tokens are handled. Allow for approximately 50KB per vCenter Server object and 4KB per workflow run.

**CAUTION** Verify that at least 1GB of free disk space is available on the machine where the Orchestrator database is located. Insufficient disk storage space might result in unwanted behavior of the Orchestrator server and client.

## Configure the Database Connection

To establish a connection to the Orchestrator database, you must configure the database connection parameters.

### Prerequisites

- Set up a new database to use with the Orchestrator server. For a list of database connection parameters, see “Database Connection Parameters,” on page 30.
- If you are using an SQL Server database, verify that the SQL Server Browser service is running.
- To store characters in the correct format in an Oracle database, set the `NLS_CHARACTER_SET` parameter to `AL32UTF8` before you configure the database connection and build the table structure for Orchestrator. This setting is crucial for an internationalized environment.

### Procedure

1. Log in to the Orchestrator configuration interface as vmware.
2. Click **Database**.
3. From the **Select the database type** drop-down menu, select the type of database for Orchestrator server to use.
4. Specify the database connection parameters.
   - If the specified parameters are correct, a message states that the connection to the database is successful.
   
   **NOTE** Although Orchestrator has established a connection to the database, the database configuration is not yet complete. You must install or update the database.

5. To build the table structure for Orchestrator, install the database.
   - After the database is populated, you can reset the database access rights to `db_dataread` and `db_datawrite`.
6. Click **Apply changes**.

The database configuration is successfully updated. On the **Database** tab, the red triangle changes to a green circle to indicate that the component is now configured correctly.

### Database Connection Parameters

To establish a connection to the database, you must specify the database connection parameters. Depending on the type of database you are connecting to, the required information might vary.

#### Table 4-1. Database Connection Parameters

<table>
<thead>
<tr>
<th>Connection Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>The user name that Orchestrator uses to connect and operate the selected database. The name you select must be a valid user on the target database with <code>db_owner</code> rights.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the user name you entered.</td>
</tr>
</tbody>
</table>
Table 4-1. Database Connection Parameters (Continued)

<table>
<thead>
<tr>
<th>Connection Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database host IP address or DNS name</td>
<td>The database server IP address or DNS name.</td>
</tr>
<tr>
<td>Port</td>
<td>The database server port that allows communication to your database.</td>
</tr>
<tr>
<td>Database name</td>
<td>The full unique name of your database. The database name is specified by the SERVICE_NAMES parameter in the initialization parameter file.</td>
</tr>
<tr>
<td>Instance name (if any)</td>
<td>The name of the database instance that can be identified by the INSTANCE_NAME parameter in the database initialization parameter file.</td>
</tr>
<tr>
<td>Domain (SQL Server only)</td>
<td>To use Windows authentication, specify the domain name of the SQL Server machine, for example company.org. To use SQL authentication, leave this text box blank.</td>
</tr>
<tr>
<td>Use Windows authentication mode (NTLMv2)</td>
<td>Select to send NTLMv2 responses when using Windows authentication. This option is valid only for SQL Server.</td>
</tr>
</tbody>
</table>

Changing SSL Certificates

By default, the Orchestrator server and Orchestrator configuration server use a self-signed SSL certificate to communicate remotely with the Orchestrator client. Orchestrator also provides an SSL certificate that controls user access to Web views.

The Orchestrator appliance uses light-httpd to run its own management site.

You can change the SSL certificates, for example if your company security policy requires you to use its SSL certificates.

For information about changing the Web views and Orchestrator client SSL certificates, see Installing and Configuring vCenter Orchestrator.

Install a Certificate from a Certificate Authority

To change an SSL certificate, you must first obtain a certificate from a CA and import it in your local keystore.

Procedure

1. Create a local certificate by running the keytool Java utility at the command prompt.
   ```bash
   keytool -genkey -alias mySslCertificate -keyalg RSA
   ```
   The keytool utility generates a file called .keystore by using the information and password that you provide when you run the command.

2. Create a certificate signing request by running the following command in the Java utility.
   ```bash
   keytool -certreq -keyalg RSA -alias mySslCertificate -file certreq.csr \ -keystore <your_keystore_filename>
   ```
   The utility generates a file called certreq.csr.

3. Submit the certreq.csr file to a certificate authority, such as VeriSign or Thawte.
   Procedures might vary from one CA to another, but they all require a valid proof of your identity.
   The CA returns a certificate that you must import.
4 Import the SSL certificate in your local keystore.
   a Download a root certificate from the CA that signed your certificate.
   b Import the root certificate in your keystore by running following command in the Java utility.
      ```sh
      keytool -import -alias root -keystore <your_keystore_filename> \
                  -trustcacerts -file <filename_of_the_root_certificate>
      ```
   c Import the SSL certificate signed by the CA (the SSL certificate must be in X509 format).
      ```sh
      keytool -import -alias mySslCertificate -keystore <your_keystore_filename> \
                  -trustcacerts -file <your_certificate_filename>
      ```

The SSL certificate is installed. You can change the Web views SSL certificate or the SSL certificate for the Orchestrator client.

**Change the Certificate of the Orchestrator Appliance Management Site**

The Orchestrator appliance uses light-httpd to run its own management site. You can change the SSL certificate of the Orchestrator appliance management site, for example if your company security policy requires you to use its SSL certificates.

**Prerequisites**

By default the Orchestrator appliance SSL certificate and private key are stored in a PEM file, which is located at: `/opt/vmware/etc/lighttpd/server.pem`. To install a new certificate, ensure that you export your new SSL certificate and private key from the Java keystore to a PEM file.

**Procedure**

1 Log in to the Orchestrator appliance Linux console as root.
2 Locate the `/opt/vmware/etc/lighttpd/lighttpd.conf` file and open it in an editor.
3 Find the following line:
   ```
   #### SSL engine
   ssl.engine = "enable"
   ssl.pemfile = "/opt/vmware/etc/lighttpd/server.pem"
   ```
4 Change the `ssl.pemfile` attribute to point to the PEM file containing your new SSL certificate and private key.
5 Save the `lighttpd.conf` file.
6 Run the following command to restart the light-httpd server.
   ```sh
   service vami-lighttp restart
   ```

You successfully changed the certificate of the Orchestrator appliance management site.

**Change the SSL Certificate of the Orchestrator Configuration Interface**

You can configure the Orchestrator configuration server to use a different SSL certificate, for example if your company security policy requires you to use their SSL certificates.

The Orchestrator configuration server stores its configuration in `jetty.xml` file, located at: `/opt/vmo/configuration/jetty/etc/jetty.xml`. To install a new SSL certificate, you must edit this file.

**Prerequisites**

Make sure that you have installed an SSL certificate signed by a CA.
Procedure

1. Log in to the Orchestrator appliance Linux console as root.

2. Encrypt your new password for the Orchestrator configuration interface.

   You can also store the password in clear text, but you should encrypt the password for security reasons.

   For example, to encrypt the password **dunesdunes** for the default user **dunes**, run the following command:

   ```
   localhost:~ # /opt/vmo/configuration/jetty/bin/jetty-password dunes dunesdunes
   dunesdunes
   OBF:1vn41w9b1wn3lw8f1vny1vn41w9b1wn3lw8f1vny
   MD5:bacfc2fc8866ec7ddb073c58bc5504b1
   CRYPT:dujEZI0nx.krc
   ```

   The encrypted password is on the line, starting with **OBF:**.

3. In the **jetty.xml** file, find the following entry:

   ```xml
   <Call name="addConnector">
     <Arg>
       <New class="org.mortbay.jetty.security.SslSocketConnector">
         <Set name="Port">8283</Set>
         <Set name="maxIdleTime">30000</Set>
         <Set name="handshakeTimeout">2000</Set>
         <Set name="keystore"><SystemProperty name="jetty.home" default="." />/etc/jssecacerts</Set>
         <Set name="password">dunesdunes</Set>
         <Set name="keyPassword">dunesdunes</Set>
         <Set name="truststore"><SystemProperty name="jetty.home" default="." />/etc/jssecacerts</Set>
         <Set name="trustPassword">dunesdunes</Set>
         <Set name="handshakeTimeout">2000</Set>
         <!-- Set name="ThreadPool">
         <!-- <New class="org.mortbay.thread.BoundedThreadPool">
         <!-- <Set name="minThreads">10</Set>
         <!-- <Set name="maxThreads">250</Set>
         <!-- </New>
         <!-- </Set -->
       </New>
     </Arg>
   </Call>
   ```

4. Change the **keystoreFile**, **truststore**, **password**, **keyPassword** and **trustPassword** attributes to refer to your .keystore file and password.

   **IMPORTANT** Type the encrypted password with the prefix **OBF:**, for example **OBF:** 1vn41w9b1wn3lw8f1vny1vn41w9b1wn3lw8f1vny.

5. Save the **jetty.xml** file.

6. Restore the default vco user credentials by running the following command:

   ```sh
   chown vco.vco /opt/vmo/configuration/jetty/etc/jetty.xml
   chmod 600 /opt/vmo/configuration/jetty/etc/jetty.xml
   ```

   **IMPORTANT** The vco user must be the owner of the **jetty.xml** file. Otherwise you cannot start the Orchestrator configuration service.

7. Restart the Orchestrator configuration server.
You successfully changed the SSL certificate for the Orchestrator configuration interface.
The Orchestrator Client and Web Operator

The Orchestrator client is an easy-to-use desktop application that you can use to perform daily administration tasks such as importing packages, running and scheduling workflows, and managing user permissions. The Orchestrator client also serves as an IDE for creating or customizing workflows.

For more information about using the Orchestrator client interface and how to create workflows, actions, packages, and other custom Orchestrator elements, see Administering VMware vCenter Orchestrator and Developing with VMware vCenter Orchestrator.

The Web operator provides an example of the orchestration functions that Web views can provide to end users in browsers, without requiring that those users use the Orchestrator client.

With the Orchestrator Web operator, you can run and monitor workflows in a Web browser without logging in to the Orchestrator client interface.

This chapter includes the following topics:

- “Log In to the Orchestrator Client,” on page 35
- “Log In to the Orchestrator Web Operator,” on page 36

Log In to the Orchestrator Client

To perform general administration tasks or to edit and create workflows, you must log in to the Orchestrator client interface.

**IMPORTANT** The Orchestrator client interface is designed for developers with administrative rights who want to develop workflows, actions, and other custom elements.

**Prerequisites**

- Download and deploy the Orchestrator appliance.
- Ensure that the appliance is up and running.

**Procedure**

1. In a Web browser, navigate to the IP address that your Orchestrator appliance virtual machine provides.
   
   http://orchestrator_appliance_ip

2. Click **Start Orchestrator Client**.

3. Type the IP or the domain name of the Orchestrator appliance in the **Host name** text box.
4 Log in by using the Orchestrator client user name and password.
   The default credentials are:
   - User name: vcoadmin
   - Password: vcoadmin

5 In the Security Warning window select an option to handle the certificate warning.
   The Orchestrator client communicates with the Orchestrator server by using an SSL certificate. A trusted
   CA does not sign the certificate during installation. You receive a certificate warning each time you connect
   to the Orchestrator server.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore</td>
<td>Continue using the current SSL certificate. The warning message appears again when you reconnect to the same Orchestrator server, or when you try to synchronize a workflow with a remote Orchestrator server.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Close the window and stop the login process.</td>
</tr>
<tr>
<td>Install this certificate and do not display any security warnings for it anymore.</td>
<td>Select this check box and click Ignore to install the certificate and stop receiving security warnings.</td>
</tr>
</tbody>
</table>

You can change the default SSL certificate with a certificate signed by a CA. For more information about
changing SSL certificates, see Installing and Configuring VMware vCenter Orchestrator.

The My Orchestrator view appears. This view summarizes the recent activities on the server, shows pending
and running workflows, running policies, scheduled tasks, completed workflows, and elements that you
recently edited.

What to do next
You can import a package, start a workflow, or set root access rights on the system. See Administering VMware
vCenter Orchestrator.

Log In to the Orchestrator Web Operator
To run and schedule workflows from the Orchestrator Web operator, you must first log in.

Prerequisites
- Download and deploy the Orchestrator appliance.
- Ensure that the appliance is up and running.

Procedure
1 In a Web browser, navigate to the IP address that your Orchestrator appliance virtual machine provides.
   http://orchestrator_appliance_ip
2 Click Web Operator.
3 Log in by using the Orchestrator user name and password.
   The default credentials are:
   - User name: vcoadmin
   - Password: vcoadmin
You see the workflow library tree and you can run and monitor workflow runs.
Index

A
assign static IP 18
audience 5

C
change the management site SSL certificate 32
change vCO appliance password 15
check-pointing 9
configuration
database connection 30
LDAP settings 28
configuring
network settings 18
Orchestrator server 21
proxy settings 18
update checks 19
configuring the vCO appliance 17

D
database
collection parameters 30
installation 29
Oracle 29
server size 29
setup 29
SQL Server 29
SQL Server Express 29
deploy the Orchestrator appliance 14
dereference links 29
download the Orchestrator appliance 14

F
filter attributes 29

I
ignore referrals 29
install updates 20

L
LDAP
browsing credentials 27
connection URL 25
LDAP Server Signing Requirements 26
lookup paths 28
SSL certificate 26
LDAP server 25
license, importing vCenter Server license 22
log in to
Linux console 14
Orchestrator client 35
Orchestrator configuration 21
Web console 17
Web operator 36

N
non-ASCII characters 30

O
Orchestrator appliance
configure for updates 19
deploy 14
download 14
overview 13
update 18
version status 18
Orchestrator architecture 11
Orchestrator client overview 35
Orchestrator configuration, log in 21
Orchestrator configuration interface, change SSL certificate 32
Orchestrator overview 9
Orchestrator plug-ins 12
Orchestrator version 13
OS 13

P
persistence 9
plug-ins configuration, vCenter Server plug-in 23, 24
policy engine 9
power on 14

S
scripting engine 9
security 9
SSL certificate 31
SSL certificates 31

T
timeouts 29
updated information 7
user roles 10

vCenter Server plug-in, install 23
vCO appliance
  change password 15
  configuring 17
versioning 9

Web console, log in 17
Web operator 35
workflow engine 9