

# Installing and Configuring VMware vCenter Orchestrator

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>.

EN-000469-01

**vmware**<sup>®</sup>

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](mailto:docfeedback@vmware.com)

Copyright © 2011 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](http://www.vmware.com)

# Contents

Installing and Configuring VMware vCenter Orchestrator	7
Updated Information	9
<b>1 Introduction to VMware vCenter Orchestrator</b>	<b>11</b>
Key Features of the Orchestrator Platform	11
Orchestrator User Types and Related Responsibilities	12
Orchestrator Architecture	13
<b>2 Orchestrator System Requirements</b>	<b>15</b>
Hardware Requirements for Orchestrator	15
Operating Systems Supported by Orchestrator	15
Supported Directory Services	15
Browsers Supported by Orchestrator	16
Orchestrator Database Requirements	16
Level of Internationalization Support	16
<b>3 Orchestrator Components Setup</b>	<b>19</b>
Orchestrator Configuration Maximums	19
vCenter Server Setup	19
Directory Services Setup	20
Orchestrator Database Setup	20
<b>4 Installing and Upgrading Orchestrator</b>	<b>21</b>
Download the vCenter Server Installer	21
Install vCenter Server and Orchestrator	22
Install Orchestrator Standalone	24
Install the Orchestrator Client on a 32-Bit Machine	25
Upgrade vCenter Server 4.1 and Orchestrator	25
Upgrade Orchestrator 4.1.x Standalone	28
Upgrading Orchestrator 4.0.x Running on a 64-Bit Machine	29
Export the Orchestrator Configuration	29
Uninstall Orchestrator	30
Install Orchestrator Standalone	30
Import the Orchestrator Configuration	31
Upgrading Orchestrator 4.0.x and Migrating the Configuration Data	31
Back Up the Orchestrator Configuration Data	32
Back Up Modified and Custom Orchestrator Elements	33
Install Orchestrator with vCenter Server on a 64-Bit Machine and Import the Configuration Data	34
Uninstall Orchestrator	36

- 5 Initial Configuration of the Orchestrator Server 37**
  - Start the Orchestrator Configuration Service 37
  - Log In to the Orchestrator Configuration Interface 38
  - Change the Default Password 39
  - Configure the Orchestrator Configuration Interface for Remote Connection 39
  - Configure the Network Connection 40
  - Orchestrator Network Ports 40
  - Import the vCenter Server SSL Certificate 42
  - Configuring LDAP Settings 42
    - Generate the LDAP Connection URL 43
    - Import the LDAP Server SSL Certificate 44
    - Specify the Browsing Credentials 45
    - Define the LDAP User and Group Lookup Paths 46
    - Define the LDAP Search Options 47
    - Common Active Directory LDAP Errors 47
  - Configuring the Orchestrator Database Connection 48
    - Configure SQL Server Express to Use with Orchestrator 48
    - Configure the Database Connection 49
    - Database Connection Parameters 50
  - Server Certificate 51
    - Create a Self-Signed Server Certificate 51
    - Obtain a Server Certificate Signed by a Certificate Authority 52
    - Import a Server Certificate 52
    - Export a Server Certificate 53
    - Changing a Self-Signed Server Certificate 53
  - Configure the Default Plug-Ins 54
    - Define the Default SMTP Connection 55
    - Configure the SSH Plug-In 55
    - Configure the vCenter Server 4.1 Plug-In 56
    - Installing a New Plug-In 57
  - Import the vCenter Server License 58
    - Access Rights to Orchestrator Server 59
  - Start the Orchestrator Server 59
  
- 6 Further Configuration Options 61**
  - Revert to the Default Password for Orchestrator Configuration 61
    - Password Encryption and Hashing Mechanism 62
  - Change the Default Configuration Ports on the Orchestrator Client Side 62
  - Uninstall a Plug-In 63
  - Activate the Service Watchdog Utility 63
  - Unwanted Server Restarts 64
  - Export the Orchestrator Configuration 64
    - Orchestrator Configuration Files 65
  - Import the Orchestrator Configuration 66
  - Configure the Maximum Number of Events and Runs 66
  - Import the Plug-In Licenses 67

- Changing SSL Certificates 67
  - Install a Certificate from a Certificate Authority 67
  - Change the Web Views SSL Certificate 68
  - Change the SSL Certificate for the Orchestrator Client 69
  - Define the Server Log Level 69

- 7 Where to Go From Here 71

- Index 73



# Installing and Configuring VMware vCenter Orchestrator

---

*Installing and Configuring VMware vCenter Orchestrator* provides information and instructions about installing, upgrading and configuring VMware® vCenter Orchestrator.

## Intended Audience

This information is intended for advanced vSphere administrators and experienced system administrators who are familiar with virtual machine technology and datacenter operations.



# Updated Information

---

*Installing and Configuring VMware vCenter Orchestrator* is updated with each release of the product or when necessary.

This table provides the update history of *Installing and Configuring VMware vCenter Orchestrator*.

Revision	Description
EN-000469-01	Updated topics <a href="#">“Operating Systems Supported by Orchestrator,”</a> on page 15 and <a href="#">“Orchestrator Database Requirements,”</a> on page 16 with the correct references to the compatibility guides.
EN-000469-00	Initial release.



# Introduction to VMware vCenter Orchestrator

---

# 1

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 11
- [“Orchestrator User Types and Related Responsibilities,”](#) on page 12
- [“Orchestrator Architecture,”](#) on page 13

## 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.

<b>Persistence</b>	Production grade external databases are used to store relevant information, such as processes, workflow states, and configuration information.
<b>Central management</b>	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.
<b>Check-pointing</b>	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.
<b>Versioning</b>	All Orchestrator Platform objects have an associated version history. This feature allows basic change management when distributing processes to different project stages or locations.

<b>Scripting engine</b>	<p>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:</p> <ul style="list-style-type: none"> <li>■ Actions</li> <li>■ Workflows</li> <li>■ Policies</li> </ul>
<b>Workflow engine</b>	<p>The workflow engine allows you to capture business processes. It uses the following objects to create a step-by-step process automation in workflows:</p> <ul style="list-style-type: none"> <li>■ Workflows and actions that Orchestrator provides.</li> <li>■ Custom building blocks created by the customer</li> <li>■ Objects that plug-ins add to Orchestrator</li> </ul> <p>Users, other workflows, a schedule, or a policy can start workflows.</p>
<b>Policy engine</b>	<p>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.</p>
<b>Web 2.0 front end</b>	<p>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.</p>
<b>Security</b>	<p>Orchestrator provides the following advanced security functions:</p> <ul style="list-style-type: none"> <li>■ Public Key Infrastructure (PKI) to sign and encrypt content imported and exported between servers</li> <li>■ Digital Rights Management (DRM) to control how exported content might be viewed, edited and redistributed</li> <li>■ Secure Sockets Layer (SSL) encrypted communications between the desktop client and the server and HTTPS access to the Web front end.</li> <li>■ Advanced access rights management to provide control over access to processes and the objects manipulated by these processes.</li> </ul>

## 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.

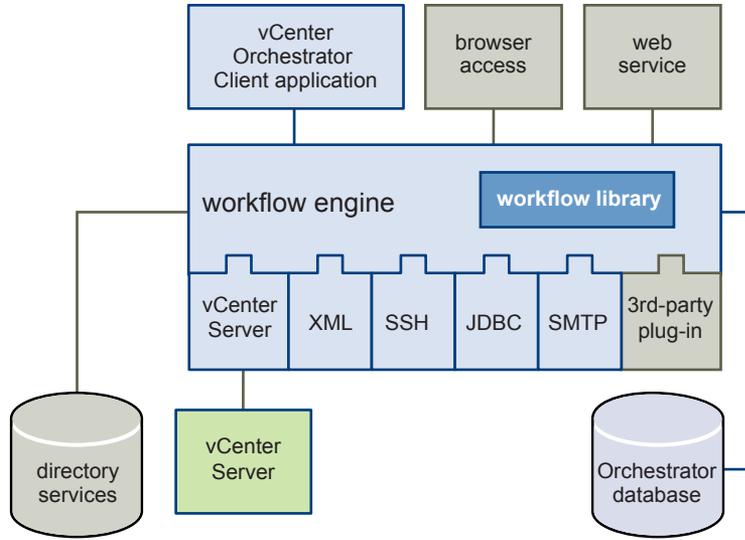
## **Orchestrator Architecture**

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.

**Figure 1-1.** VMware vCenter Orchestrator Architecture



# Orchestrator System Requirements

---

Your system must meet the technical requirements that are necessary to install and configure Orchestrator.

For a list of the supported versions of vCenter Server, see [VMware Product Interoperability Matrix](#).

This chapter includes the following topics:

- [“Hardware Requirements for Orchestrator,”](#) on page 15
- [“Operating Systems Supported by Orchestrator,”](#) on page 15
- [“Supported Directory Services,”](#) on page 15
- [“Browsers Supported by Orchestrator,”](#) on page 16
- [“Orchestrator Database Requirements,”](#) on page 16
- [“Level of Internationalization Support,”](#) on page 16

## Hardware Requirements for Orchestrator

Verify that your system meets the minimum hardware requirements before you install Orchestrator.

- 2.0GHz or faster Intel or AMD x86 processor. At least two CPUs are recommended. Processor requirements might differ if your database runs on the same hardware.
- 4GB RAM. You might need more RAM if your database runs on the same hardware.
- 2GB disk space. You might need more storage if your database runs on the same hardware.
- A free static IP address.

## Operating Systems Supported by Orchestrator

You can install the Orchestrator 4.2 server only on 64-bit operating systems.

For a list of the operating systems supported by Orchestrator, see the *VMware Compatibility Guide* at <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17>.

## Supported Directory Services

Orchestrator requires a working LDAP server.

Orchestrator supports these directory service types.

- Windows Server 2003 Active Directory
- Windows Server 2008 Active Directory
- Novell eDirectory Server 8.8.3

- Sun Java System Directory Server 6.3

## Browsers Supported by Orchestrator

The Orchestrator configuration interface and Web views require a Web browser.

You must have one of the following browsers to connect to the Orchestrator configuration interface and Web views.

- Microsoft Internet Explorer 7.0
- Mozilla Firefox 3.0 (build 3.0.6 or later)
- Mozilla Firefox 3.5

## Orchestrator Database Requirements

Orchestrator requires a database that is separate from the standard vCenter Server database. For small-scale deployments, you can use the SQL Server Express database that is bundled with vCenter Server.

---

**NOTE** To ensure efficient CPU and memory usage, you should consider hosting the Orchestrator database and the Orchestrator server on different machines. Verify that at least 1GB of free disk space is available on each machine.

---

For a list of the databases supported by Orchestrator, see the *VMware Product Interoperability Matrixes* at [http://partnerweb.vmware.com/comp\\_guide2/sim/interop\\_matrix.php](http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php).

## Level of Internationalization Support

Orchestrator is compliant with i18n level 1.

### Non-ASCII Character Support in Orchestrator

Although Orchestrator is not localized, it can run on a non-English operating system and handle non-English text.

**Table 2-1.** Non-ASCII Character Support in Orchestrator GUI

Support for Non-ASCII Characters				
Item	Description Field	Name Field	Input and Output Parameters	Attributes
Action	Yes	No	No	No
Folder	Yes	Yes	-	-
Configuration element	Yes	Yes	-	No
Package	Yes	Yes	-	-
Policy	Yes	Yes	-	-
Policy template	Yes	Yes	-	-
Resource element	Yes	Yes	-	-
Web view	Yes	Yes	-	No
Workflow	Yes	Yes	No	No
Workflow presentation display group and input step	Yes	Yes	-	-

## Non-ASCII Character Support for Oracle Databases

To store characters in the correct format in an Oracle database, set the `NLS_CHARACTER_SET` parameter to `AL32UTF8` before configuring the database connection and building the table structure for Orchestrator. This setting is crucial for an internationalized environment.



# Orchestrator Components Setup

---

To enhance the availability and scalability of your Orchestrator setup, install Orchestrator on a computer different from the computer on which vCenter Server runs. With such separation, you can adjust the operating system to meet the specific recommendations for each service.

This chapter includes the following topics:

- [“Orchestrator Configuration Maximums,”](#) on page 19
- [“vCenter Server Setup,”](#) on page 19
- [“Directory Services Setup,”](#) on page 20
- [“Orchestrator Database Setup,”](#) on page 20

## Orchestrator Configuration Maximums

When you configure Orchestrator, verify that you stay at or below the supported maximums.

**Table 3-1.** Orchestrator Configuration Maximums

Item	Maximum
Connected vCenter Server systems	10
Connected ESX/ESXi servers	300
Connected virtual machines spread over vCenter Server systems	15000
Concurrent running workflows	150

## vCenter Server Setup

Increasing the number of vCenter Server instances in your Orchestrator setup causes Orchestrator to manage more sessions. Each active session results in activity on the corresponding vCenter Server, and too many active sessions can cause Orchestrator to experience timeouts when more than 10 vCenter Server connections occur.

For a list of the supported versions of vCenter Server, see [VMware Product Interoperability Matrix](#).

---

**NOTE** You can run multiple vCenter Server instances on different virtual machines in your Orchestrator setup if your network has sufficient bandwidth and latency. If you are using LAN to improve the communication between Orchestrator and vCenter Server, a 100Mb line is mandatory.

---

## Directory Services Setup

Orchestrator requires a connection to an LDAP server.

Orchestrator supports the following directory service types: Active Directory, eDirectory, and Sun Java System Directory Server.

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 narrow 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.

## Orchestrator Database Setup

Orchestrator requires a database to store workflows and actions.

Orchestrator server supports Oracle and Microsoft SQL Server databases. Orchestrator can work with Microsoft SQL Server Express in small-scale environments consisting of up to 5 hosts and 50 virtual machines.

For details about using SQL Server Express with Orchestrator, see [“Configure SQL Server Express to Use with Orchestrator,”](#) on page 48.

The common workflow for setting up the Orchestrator database is the following:

- 1 Create a new database. For more information about creating a new database, refer to the documentation of your database provider (Microsoft or Oracle).
- 2 Enable the database for remote connection. For an example of how to do that, see [“Configure SQL Server Express to Use with Orchestrator,”](#) on page 48.
- 3 Configure the database connection parameters. For more information, see [“Configure the Database Connection,”](#) on page 49.

The way in which your database is set up can affect Orchestrator performance. Install the database on a machine other than the one on which the Orchestrator server is installed. This method avoids the JVM and DB server having to share CPU, RAM, and I/Os.

Storing your database plug-ins in a database separate from the one that Orchestrator uses results in more modularity when upgrading the system. A dedicated database instance allows you to perform upgrades and maintenance without impacting other products.

The location of the database is important because almost every activity on the Orchestrator server triggers operations on the database. To avoid latency in the database connection, connect to the database server that is closest to your Orchestrator server and that is on the network with the highest bandwidth.

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 installed and on the machine where the Orchestrator server is installed.

Insufficient disk storage space might result in unwanted behavior of the Orchestrator server and client.

---

# Installing and Upgrading Orchestrator

---

Orchestrator consists of a server component and a client component. You can install the Orchestrator components on the machine on which vCenter Server is installed or on a separate machine. To improve performance, install the Orchestrator server component on a separate machine.

---

**IMPORTANT** You can install the Orchestrator configuration server on 64-bit Windows machines only. The Orchestrator client can run on both 32-bit and 64-bit Windows machines.

---

To install Orchestrator, you must be either a local Administrator or a domain user that is a member of the Administrators group.

This chapter includes the following topics:

- [“Download the vCenter Server Installer,”](#) on page 21
- [“Install vCenter Server and Orchestrator,”](#) on page 22
- [“Install Orchestrator Standalone,”](#) on page 24
- [“Install the Orchestrator Client on a 32-Bit Machine,”](#) on page 25
- [“Upgrade vCenter Server 4.1 and Orchestrator,”](#) on page 25
- [“Upgrade Orchestrator 4.1.x Standalone,”](#) on page 28
- [“Upgrading Orchestrator 4.0.x Running on a 64-Bit Machine,”](#) on page 29
- [“Upgrading Orchestrator 4.0.x and Migrating the Configuration Data,”](#) on page 31
- [“Uninstall Orchestrator,”](#) on page 36

## Download the vCenter Server Installer

You must download the installer for vCenter Server, the vSphere Client, and associated vCenter components and support tools.

### Procedure

- 1 Download the zip file for vCenter Server from the VMware downloads page at <http://www.vmware.com/support/>.
- 2 Extract the files from the zip archive.

## Install vCenter Server and Orchestrator

When you install vCenter Server 5.0, Orchestrator 4.2 is silently installed on your system as an additional component.

### Prerequisites

- Verify that the machine on which you are installing vCenter Server 5.0 is a 64-bit operating system platform.
- Verify that you have the Microsoft .NET 3.5 SP1 Framework installed. If your system does not have it installed, the vCenter Server installer installs it. The .NET 3.5 SP1 installation might require Internet connectivity to download additional files.
- For a list of required ports, see the *vSphere Installation and Setup* documentation.
- Make sure that your system meets the vCenter Server installation requirements. For more information about the vCenter Server installation prerequisites, see the *vSphere Installation and Setup* documentation.
- Download the vCenter Server 5.0 installer from the VMware Web site.

### Procedure

- 1 Start the vCenter Server installer.

In the software installer directory, for example, `C:\install_directory\`, double-click the `autorun.exe` file.

- 2 Select **vCenter Server™** and click **Install**.

- 3 Follow the prompts in the installation wizard to choose the installer language, agree to the end user patent and license agreements, enter your user name, organization name, and license key.

If you omit the license key, vCenter Server will be in evaluation mode, which allows you to use the full feature set for a 60-day evaluation period. After installation, you can enter the license key to convert vCenter Server to licensed mode.

- 4 Choose the type of database that you want to use.

Option	Action
<b>Install SQL Server 2008 Express instance (for small-scale deployments)</b>	Select <b>Install SQL Server 2008 Express instance (for small-scale deployments)</b> to use the bundled database. The SQL Server Express database is suitable for deployments of up to 5 hosts and 50 virtual machines.
<b>Use an existing supported database</b>	Select <b>Use an existing supported database</b> option to use an existing database. Select your database from the list of available DSNs. Type the user name and password for the DSN. If your database uses Windows NT authentication, the user name and password fields are disabled.

**NOTE** A dialog box might appear, warning you that the DSN points to an older version of a repository that must be upgraded. If you click **Yes**, the installer upgrades the database schema, making the database irreversibly incompatible with previous vCenter Server versions. For more information, see the *vSphere Upgrade* documentation.

- 5 Set the login information for vCenter Server.
  - If you are using a nonbundled database, specify the administrator name and password that you use when you log in to the system on which you are installing vCenter Server.
  - If you are using the bundled SQL Server database, select **Use SYSTEM Account**.

You will need the user name and password entered here to log in to vCenter Server after install it.

The Fully Qualified Domain Name field displays the FQDN of the system on which you are installing vCenter Server. The vCenter Server installer checks that the FQDN is resolvable. If not, a warning message is displayed when you click **Next**. Change the entry to a resolvable FQDN. You must enter the FQDN, not the IP address.

- 6 Either accept the default destination folders or click **Change** to select another location, and click **Next**.  
The installation path cannot have commas (,) or periods (.).

---

**NOTE** To install the vCenter Server on a drive other than C:, verify that the C:\WINDOWS\Installer folder is large enough to accommodate the Microsoft Windows Installer .msi file. If the folder is not large enough, your vCenter Server installation might fail.

---

- 7 Select **Create a standalone VMware vCenter Server instance** or **Join Group**.

Join a Linked Mode group to enable the vSphere Client to view, search, and manage data across multiple vCenter Server systems. For more information, see the *vSphere Installation and Setup* documentation. .

---

**NOTE** You cannot join a Linked Mode group during the installation if you are upgrading the VirtualCenter or vCenter Server database schema. You can join a Linked Mode group after the installation is complete.

---

- 8 If you join a group, enter the fully qualified domain name and LDAP port number of any remote vCenter Server system and click **Next**.

In some cases, you can enter the IP address instead of the fully qualified domain name. To help ensure connectivity, the best practice is to use the fully qualified domain name. For IPv6, unless both the local and the remote machine are in IPv6 mode, you must enter the fully qualified domain name of the remote machine instead of the IPv6 address. If the local machine has an IPv4 address and the remote machine has an IPv6 address, the local machine must support IPv4 and IPv6 mixed mode. The domain name server must be able to resolve both IPv4 and IPv6 addresses if your environment has both addressing types in a single Linked Mode group.

- 9 Specify the port numbers to use or accept the default port numbers and click **Next**.
- 10 Select the amount of JVM memory to allocate for vCenter Server Web services, according to the size of your inventory.

This setting determines the JVM heap settings for Tomcat, Inventory Service, and Storage Based Policy Management (SPS) services. You can adjust this setting after installation if the number of hosts in your environment changes.

- 11 In the Ready to Install the Program window, select **Select to bump up the ephemeral port value**.

This option increases the number of available ephemeral ports. If your vCenter Server manages hosts on which you will power on more than 2000 virtual machines simultaneously, this option prevents the pool of available ephemeral ports from being exhausted.

- 12 Click **Install**.

Installation might take several minutes. Multiple progress bars appear during the installation of the selected components.

- 13 Click **Finish**.

You completed the installation of vCenter Server. The Orchestrator client and server components are installed on your system.

### What to do next

Start the VMware vCenter Orchestrator Configuration service and log in to the Orchestrator configuration interface at: <http://localhost:8282>.

Configure Orchestrator using an IPv4 operating system. Orchestrator does not support IPv6 operating systems.

## Install Orchestrator Standalone

For production environments and to enhance the scalability of your Orchestrator setup, install Orchestrator on a dedicated Windows machine.

You can install the Orchestrator server only on a 64-bit operating system platform.

The Orchestrator client can run on both 32-bit and 64-bit Windows machines.

You can install the Orchestrator client on a 32-bit machine. For more information, see [“Install the Orchestrator Client on a 32-Bit Machine,”](#) on page 25.

---

**NOTE** If you try to install Orchestrator 4.2 on a 64-bit machine on which an instance of Orchestrator 4.0.x is running, the 64-bit installer does not detect the earlier version of Orchestrator. As a result, two versions of Orchestrator are installed and coexist.

---

### Prerequisites

- Verify that your hardware meets the Orchestrator system requirements. See [“Hardware Requirements for Orchestrator,”](#) on page 15.
- Download the vCenter Server 5.0 installer from the VMware Web site.

### Procedure

- 1 Start the Orchestrator installer.

In the software installer directory, browse to the C:\*install\_directory*\vCenter-Server\vCO\ folder and double-click vCenterOrchestrator.exe.

The file contains installers for the client and the server components.

- 2 Click **Next**.
- 3 Accept the terms in the license agreement and click **Next**.
- 4 Either accept the default destination folders or click **Change** to select another location, and click **Next**.



**CAUTION** You cannot install Orchestrator in a directory whose name contains non-ASCII characters. If you are operating in a locale that features non-ASCII characters, you must install Orchestrator in the default location.

- 5 Select the type of installation and click **Next**.

Option	Description
<b>Client</b>	Installs the Orchestrator client application, which allows you to create and edit workflows.
<b>Server</b>	Installs the Orchestrator server platform.
<b>Client-Server</b>	Installs the Orchestrator client and server.

- 6 Specify the location for the Orchestrator shortcuts and click **Next**.



**CAUTION** The name of the shortcuts directory must contain only ASCII characters.

- 7 Click **Install** to complete the installation process.
- 8 Click **Done** to close the installer.

**What to do next**

To start configuring Orchestrator, verify that the VMware vCenter Orchestrator Configuration service is running and log in to the Orchestrator configuration interface at: <http://localhost:8282>.

**Install the Orchestrator Client on a 32-Bit Machine**

The Orchestrator client is a desktop application that allows you to import packages, run and schedule workflows, and manage user permissions. If you install vCenter Server, the Orchestrator client is installed silently on your system. You can install the Orchestrator client on a 32-bit machine.

You can use the standalone Orchestrator client installer on a 32-bit machine only.

**Prerequisites**

Download the Orchestrator client 32-bit installer from the VMware Web site.

**Procedure**

- 1 Log in to the 32-bit machine as an administrator.
- 2 Double-click the vCenter Orchestrator Client distribution file and click **Next**.  
The filename is `vCenterOrchestratorClient-4.a.b.-yyy.exe`, where *a* and *b* are major and minor version, and *yyy* is the build number.
- 3 Accept the terms in the license agreement and click **Next**.
- 4 Either accept the default destination folders or click **Change** to select another location, and click **Next**.



**CAUTION** You cannot install Orchestrator in a directory whose name contains non-ASCII characters. If you are operating in a locale that features non-ASCII characters, you must install Orchestrator in the default location.

- 5 Specify the location for the Orchestrator shortcuts and click **Next**.



**CAUTION** The name of the shortcuts directory must contain only ASCII characters.

- 6 Review the summary and click **Next**.
- 7 Click **Install** to complete the installation process.
- 8 Click **Done** to close the installer.

The Orchestrator client component is installed on your system.

**What to do next**

You can log in to the Orchestrator client interface and perform general administration tasks and create workflows.

**Upgrade vCenter Server 4.1 and Orchestrator**

If you have installed Orchestrator 4.1.x with the vCenter Server 4.1.x installer on a 64-bit machine, you can upgrade to the latest version of Orchestrator by upgrading your vCenter Server on the same machine. The vCenter Server 5.0 installer detects the previous version and the installation path.

This procedure requires downtime for the Orchestrator and vCenter Server system that you are upgrading. You do not need to power off virtual machines.

## Prerequisites

- Verify that the vCenter Server upgrade prerequisites and database upgrade prerequisites are met. For more information about preparing for the upgrade of vCenter Server, see the *vSphere Upgrade* documentation.
- Verify that you know the correct port numbers to use. For a list of required ports, see the *vSphere Installation and Setup* documentation.
- Download the vCenter Server 5.0 installer from the VMware Web site.
- Back up your vCenter Server environment. For more information, see the *vSphere Upgrade* documentation.
- Log in as Administrator on the Windows machine on which you are performing the upgrade.

## Procedure

- 1 Stop the Orchestrator Server and the vCenter Server services.
  - a Click **Start > Programs > Administrative Tools > Services**.
  - b In the right pane, right-click **VMware vCenter Orchestrator Server** and select **Stop**.
  - c In the right pane, right-click **VMware vCenter Orchestrator Configuration** and select **Stop**.
  - d In the right pane, right-click **VMware VirtualCenter Server** and select **Stop**.
- 2 Start the vCenter Server installer.  
In the software installer directory, double-click `autorun.exe`.
- 3 Select **vCenter Server™** and click **Install**.
- 4 Follow the prompts in the installation wizard to choose the installer language, agree to the end user patent and license agreements, enter your user name, organization name, and license key.  
  
If you omit the license key, vCenter Server will be in evaluation mode, which allows you to use the full feature set for a 60-day evaluation period. After installation, you can enter the license key to convert vCenter Server to licensed mode.
- 5 Select the DSN.  
  
This page appears if the installer is unable to determine the DSN for the database to be upgraded. The DSN must be a 64-bit DSN. Depending on the database type, the DSN might already be selected, or only one option might be available.
- 6 Specify the database user name and password for the DSN and click **Next**.  
  
You can omit the database user name and password if the DSN is using Windows NT authentication.  
  
If you specify a remote SQL Server database that uses Windows NT authentication, the database user and the logged-in user on the vCenter Server machine must be the same.
- 7 Select whether to upgrade the vCenter Server database.
  - Select **Upgrade existing vCenter Server database** to continue with the upgrade of vCenter Server.
  - Select **Do not upgrade existing vCenter Server database** if you do not have a backup copy of your database.  
  
You cannot continue with the upgrade.
- 8 Select **I have taken a backup of the existing vCenter Server database and SSL certificates** and click **Next**.

- 9 Select how to upgrade vCenter Agent and click **Next**.

Option	Description
<b>Automatic</b>	vCenter Agent is upgraded on all hosts in the vCenter Server inventory.
<b>Manual</b>	<p>All hosts are disconnected from vCenter Server. To upgrade vCenter Agent, reconnect the host to vCenter Server.</p> <p>Select this option if one of the following situations:</p> <ul style="list-style-type: none"> <li>■ You need to control the timing of vCenter Agent upgrades on specific hosts.</li> <li>■ The number of hosts in the vCenter Server inventory is large, and you anticipate that upgrading vCenter Agent on all hosts would negatively affect vCenter Server performance.</li> </ul>

vCenter Agent is installed on each host in the inventory to enable vCenter Server to manage the host. vCenter Agent must be upgraded when vCenter Server is upgraded.

- 10 Set the login information for vCenter Server.

Option	Action
<b>SYSTEM Account</b>	Select the <b>Use SYSTEM account</b> checkbox, type the fully qualified domain name of the vCenter Server host, and click <b>Next</b> . You cannot use the SYSTEM account if you are using the bundled database or SQL Server with Windows authentication.
<b>User-specified account</b>	Deselect the <b>Use SYSTEM account</b> checkbox, type the account password and the fully qualified domain name of the vCenter Server host and click <b>Next</b> .

- 11 Select a folder to install vCenter Inventory Service.

**NOTE** The folder size might grow large.

- 12 Specify the port numbers to use or accept the port numbers that were used in the previous vCenter Server installation and click **Next**.
- 13 Select the amount of memory to allocate to the vCenter JVM in Tomcat, according to the number of hosts in your environment.
- You can adjust this setting after installation if the number of hosts in your environment changes.
- 14 In the Ready to Install the Program page, select the check box to enhance the number of ephemeral ports available for transactions and click **Install**.
- 15 Click **Finish**.
- 16 Start the Orchestrator configuration service and log in to the Orchestrator configuration interface.
- 17 On the **Database** tab, update the database by clicking **Update database**.
- 18 Reimport the SSL certificate for the licensed vCenter Server and start the Orchestrator server.

For more information about importing the vCenter Server SSL certificate, see [“Import the vCenter Server SSL Certificate,”](#) on page 42.

You upgraded vCenter Server and the Orchestrator client and server components. The existing Orchestrator configuration is preserved.

## Upgrade Orchestrator 4.1.x Standalone

To upgrade Orchestrator 4.1.x on a 64-bit Microsoft Windows machine that is different from the machine on which vCenter Server runs, start the latest version of the Orchestrator standalone installer.

### Prerequisites

- Create a backup of the Orchestrator database.
- Export the Orchestrator configuration to a local file. See [“Export the Orchestrator Configuration,”](#) on page 29.
- Export your custom workflows and packages. See [“Back Up Modified and Custom Orchestrator Elements,”](#) on page 33.
- Log in as Administrator to the Windows machine on which you are performing the upgrade.
- Download the vCenter Server 5.0 installer from the VMware Web site.

### Procedure

- 1 Stop the Orchestrator server service.
  - a Select **Start > Programs > Administrative Tools > Services**.
  - b In the right pane, right-click **VMware vCenter Orchestrator Server** and select **Stop**.
  - c In the right pane, right-click **VMware vCenter Orchestrator Configuration** and select **Stop**.

- 2 Start the Orchestrator installer.

In the software installer directory, browse to the C:\*install\_directory*\vCenter-Server\vCO\ folder and double-click vCenterOrchestrator.exe.

The file contains installers for the client and the server components.

- 3 Click **Next**.
- 4 Accept the terms in the license agreement and click **Next**.
- 5 Select **Continue with update** to upgrade Orchestrator.
- 6 When the installer detects the installation directory, click **Next**.

You cannot change the installation directory when you are upgrading Orchestrator. To change this parameter, you must perform a fresh installation.

- 7 Select the type of upgrade that matches your existing installation type and click **Next**.

Option	Description
<b>Client</b>	Upgrades the Orchestrator client application, which allows you to create and edit workflows.
<b>Server</b>	Upgrades the Orchestrator server platform.
<b>Client-Server</b>	Upgrades the Orchestrator client and server.

For example, if you installed only the Orchestrator client, select **Client** and then upgrade your Orchestrator server separately.

---

**IMPORTANT** The versions of the Orchestrator client and server must be the same.

---

- 8 Specify the location for the Orchestrator shortcuts and click **Next**.



**CAUTION** The name of the shortcuts directory must contain only ASCII characters.

---

- 9 Click **Install** to complete the installation process.
- 10 Click **Done** to close the installer.
- 11 Start the Orchestrator configuration service and log in to the Orchestrator configuration interface.
- 12 On the **Database** tab, update the database by clicking **Update database**.
- 13 Reimport the SSL certificate for the licensed vCenter Server and start the Orchestrator server.

For more information about importing the vCenter Server SSL certificate, see [“Import the vCenter Server SSL Certificate,”](#) on page 42.

You upgraded to the latest version of Orchestrator. The existing Orchestrator configuration is preserved.

## Upgrading Orchestrator 4.0.x Running on a 64-Bit Machine

If vCenter Orchestrator 4.0.x is installed on the same 64-bit machine as vCenter Server 4.0 and the later update releases, you cannot upgrade Orchestrator by upgrading to vCenter Server 5.0. VMware does not support the in-place upgrade of a standalone Orchestrator instance running on a 64-bit machine.

To upgrade to Orchestrator 4.2, you must export the Orchestrator configuration settings, uninstall the existing Orchestrator instance, run the Orchestrator installer, and import the configuration settings.

- 1 [Export the Orchestrator Configuration](#) on page 29

The Orchestrator configuration interface provides a mechanism to export the Orchestrator configuration settings to a local file. This mechanism allows you to take a snapshot of your system configuration at any moment and import this configuration into a new Orchestrator instance.

- 2 [Uninstall Orchestrator](#) on page 30

You can remove the Orchestrator client and server components from your system by using **Add or Remove Programs**.

- 3 [Install Orchestrator Standalone](#) on page 30

For production environments and to enhance the scalability of your Orchestrator setup, install Orchestrator on a dedicated Windows machine.

- 4 [Import the Orchestrator Configuration](#) on page 31

You can restore the previously exported system configuration if a system failure occurs or when you reinstall Orchestrator.

### Export the Orchestrator Configuration

The Orchestrator configuration interface provides a mechanism to export the Orchestrator configuration settings to a local file. This mechanism allows you to take a snapshot of your system configuration at any moment and import this configuration into a new Orchestrator instance.

You should export and save your configuration settings on a regular basis, especially when making modifications, performing maintenance, or upgrading the system.

For a list of exported configuration settings, see [“Orchestrator Configuration Files,”](#) on page 65.

#### Procedure

- 1 Log in to the Orchestrator configuration interface as **vmware**.
- 2 On the **General** tab, click **Export Configuration**.
- 3 (Optional) Type a password to protect the configuration file.  
Use the same password when you import the configuration.
- 4 Click **Export**.

- 5 Click **Save** when prompted.

Orchestrator creates a `vmo_config_dateReference.vmoconfig` file which you can use to clone or to restore the system.

## Uninstall Orchestrator

You can remove the Orchestrator client and server components from your system by using **Add or Remove Programs**.

### Prerequisites

- Save the Orchestrator configuration settings to a local file. For more details, see [“Export the Orchestrator Configuration,”](#) on page 29.
- Back up custom workflows and plug-ins.

### Procedure

- 1 From the Windows **Start** menu, select **Settings > Control Panel > Add or Remove Programs**.
- 2 Select **vCenter Orchestrator** and click **Remove**.
- 3 Click **Uninstall** in the Uninstall vCenter Orchestrator window.

A message confirms that all items have been successfully removed.

- 4 Click **Done**.

Orchestrator is uninstalled from your system.

## Install Orchestrator Standalone

For production environments and to enhance the scalability of your Orchestrator setup, install Orchestrator on a dedicated Windows machine.

You can install the Orchestrator server only on a 64-bit operating system platform.

The Orchestrator client can run on both 32-bit and 64-bit Windows machines.

You can install the Orchestrator client on a 32-bit machine. For more information, see [“Install the Orchestrator Client on a 32-Bit Machine,”](#) on page 25.

---

**NOTE** If you try to install Orchestrator 4.2 on a 64-bit machine on which an instance of Orchestrator 4.0.x is running, the 64-bit installer does not detect the earlier version of Orchestrator. As a result, two versions of Orchestrator are installed and coexist.

---

### Prerequisites

- Verify that your hardware meets the Orchestrator system requirements. See [“Hardware Requirements for Orchestrator,”](#) on page 15.
- Download the vCenter Server 5.0 installer from the VMware Web site.

### Procedure

- 1 Start the Orchestrator installer.

In the software installer directory, browse to the `C:\install_directory\vCenter-Server\vCO\` folder and double-click `vCenterOrchestrator.exe`.

The file contains installers for the client and the server components.

- 2 Click **Next**.
- 3 Accept the terms in the license agreement and click **Next**.

- 4 Either accept the default destination folders or click **Change** to select another location, and click **Next**.



**CAUTION** You cannot install Orchestrator in a directory whose name contains non-ASCII characters. If you are operating in a locale that features non-ASCII characters, you must install Orchestrator in the default location.

- 5 Select the type of installation and click **Next**.

Option	Description
<b>Client</b>	Installs the Orchestrator client application, which allows you to create and edit workflows.
<b>Server</b>	Installs the Orchestrator server platform.
<b>Client-Server</b>	Installs the Orchestrator client and server.

- 6 Specify the location for the Orchestrator shortcuts and click **Next**.



**CAUTION** The name of the shortcuts directory must contain only ASCII characters.

- 7 Click **Install** to complete the installation process.
- 8 Click **Done** to close the installer.

#### What to do next

To start configuring Orchestrator, verify that the VMware vCenter Orchestrator Configuration service is running and log in to the Orchestrator configuration interface at: <http://localhost:8282>.

## Import the Orchestrator Configuration

You can restore the previously exported system configuration if a system failure occurs or when you reinstall Orchestrator.

#### Procedure

- 1 Log in to the Orchestrator configuration interface as **vmware**.
- 2 On the **General** tab, click **Import Configuration**.
- 3 Type the password you used when exporting the configuration.  
This step is not necessary, if you have not specified a password.
- 4 Browse to select the `.vmoconfig` file you exported from your previous installation.
- 5 Click **Import**.

A message states that the configuration is successfully imported. The new system replicates the old configuration completely.

## Upgrading Orchestrator 4.0.x and Migrating the Configuration Data

If your Orchestrator 4.0.x is installed on a 32-bit machine, you might want to migrate your Orchestrator data to a 64-bit machine and then perform an upgrade to a later version.

The vCenter Server 5.0 installation media includes a data migration tool that you can use to migrate Orchestrator and vCenter Server configuration data from a 32-bit vCenter Server machine to a 64-bit machine. You can find the data migration tool in `C:\install_directory\datamigration`.

For detailed instructions about migrating the vCenter Server configuration and database, see the *vSphere Upgrade* documentation.

You can migrate the following Orchestrator configuration data with the data migration tool:

- Network configuration settings
- LDAP connection data
- Database connection data
- SSL certificates
- Licenses
- vCenter Server plug-in configuration data
- Mail plug-in configuration data
- SSH plug-in configuration data

The Orchestrator database is not migrated. Your new Orchestrator instance accesses the existing database if it is running on a dedicated database server. If you are upgrading from vCenter Orchestrator 4.0, you must update the database from the **Database** tab of the Orchestrator configuration interface.

If your Orchestrator database is local to the Orchestrator server, it becomes inaccessible after the configuration backup because the 64-bit machine uses the IP address and host name of the source machine. You must set up a new database and configure the database connection from the **Database** tab of the Orchestrator configuration interface.

## Back Up the Orchestrator Configuration Data

Use the data migration tool that is included in the vCenter Server installation media to back up the existing Orchestrator configuration and restore it to a new Orchestrator instance.

Migrating Orchestrator configuration settings by using the data migration tool is only possible when Orchestrator is installed silently with vCenter Server. For instructions about migrating configuration settings for a standalone Orchestrator instance, see [“Export the Orchestrator Configuration,”](#) on page 29 and [“Import the Orchestrator Configuration,”](#) on page 31.

For detailed information about backing up and restoring the existing vCenter Server database and configuration, see the *vSphere Upgrade* documentation.

### Prerequisites

- Log in to the 32-bit source machine as an administrator.
- Verify that vCenter Orchestrator 4.0 or an update release is installed and configured.
- Stop the VMware vCenter Orchestrator Configuration, VMware vCenter Orchestrator Server, and VMware VirtualCenter Server services.
- If the `\datamigration\data\` folder already exists from a previous backup attempt, backup cannot proceed. Remove or rename this folder before backing up the Orchestrator configuration.

### Procedure

- 1 Start the vCenter Server installer.  
In the software installer directory, double-click the `autorun.exe` file.
- 2 Click **Explore media**.
- 3 Open the `datamigration` folder and extract the `datamigration.zip` archive to a writeable local file system on the source machine.
- 4 From the Windows command prompt, navigate to the `datamigration` folder, type **backup.bat**, and press Enter to run the backup script of the data migration tool.

- 5 Respond to the script prompts.

The script checks the vCenter Server version, database type, VMware vCenter Update Manager configuration (if installed), and Orchestrator configuration to determine whether they are compatible with the data migration tool.

- 6 Check `\logs\backup.log` in the `datamigration` folder for errors.

- If you find no errors, the data backup was successful.
- If you find errors, correct the source of the error and rerun `backup.bat`.

The existing Orchestrator configuration is successfully exported. The file that stores the system settings is named `vco.backup.vmoconfig` and is located in the `datamigration\data\vco` folder.

### What to do next

Back up any standard Orchestrator elements that you modified. During the database upgrade, elements with a higher version number silently overwrite the existing elements. See [“Back Up Modified and Custom Orchestrator Elements,”](#) on page 33.

## Back Up Modified and Custom Orchestrator Elements

When you upgrade Orchestrator, elements with a higher version number silently overwrite the elements stored in the Orchestrator database.

For example, if you have edited any standard workflows, actions, policies, Web views, or configuration elements and you import a package containing the same elements with a higher version number, your changes to the elements are lost. To make modified and custom elements available after the upgrade, you must export them in a package before you start the upgrade procedure.

### Procedure

- 1 Log in to the Orchestrator client application.
- 2 Create a package that contains all the Orchestrator elements that you created or edited.
  - a In the Orchestrator client, click the **Packages** view.
  - b Click the menu button in the title bar of the **Packages** list and select **Add package**.
  - c Name the new package and click **OK**.  
 The syntax for package names is *domain.your\_company.folder.package\_name*. For example, `com.vmware.myfolder.mypackage`.
  - d Right-click the package and select **Edit**.
  - e Add a description for the package in the **General** tab.
  - f From the **Workflows** tab add workflows to the package.
  - g (Optional) Click the **Policies**, **Actions**, **Web View**, **Configurations**, **Resources**, and **Used Plug-Ins** tabs to add policy templates, actions, Web views, configuration elements, resource elements, and plug-ins to the package.
- 3 Export the package.
  - a Right-click the package to export and select **Export package**.
  - b Browse to select a location in which to save the package and click **Open**.
  - c (Optional) Sign the package with a specific certificate.
  - d (Optional) Impose restrictions on the exported package.

- e (Optional) Deselect the **Export version history** check box if you do not want to export the version history of the package.
- f Click **Save**.

The upgrade procedure cannot affect the Orchestrator elements that you modified or created.

### What to do next

You can upgrade Orchestrator and restore the configuration by using the data migration tool. After the upgrade, import the package that contains your custom elements and confirm the import of elements with lower version numbers. For details about importing a package, see *Administering VMware vCenter Orchestrator*.

## Install Orchestrator with vCenter Server on a 64-Bit Machine and Import the Configuration Data

When you install vCenter Server, Orchestrator is silently installed on your system as an additional component. You can use the data migration tool to launch the vCenter Server installer, install Orchestrator, and import the configuration from your previous Orchestrator installation.

For detailed information about installing vCenter Server 5.0 and restoring the existing vCenter Server database and configuration, see the *vSphere Upgrade* documentation.

### Prerequisites

- Log in to the 64-bit machine as an administrator.
- For the 64-bit machine, use the same IP address and host name as that which you used for the source 32-bit machine.
- Ensure that the destination machine has Microsoft Windows Installer (MSI) 4.5 installed on it.
- Download the vCenter Server installer.

### Procedure

- 1 Copy the `datamigration` folder from the source machine to the destination machine.
- 2 Insert the vCenter Server installation media into the DVD-ROM drive on the destination machine, or copy the installation ISO image to the destination machine.
- 3 From the Windows command prompt, navigate to the `datamigration` folder you copied from the source machine, type `install.bat` and press Enter.
- 4 If the name of the destination machine is different from the name of the source machine, type `y` to continue.
- 5 Type the path to the vCenter Server 5.0 installation media and press Enter.  
The install script verifies that migration data is present, and starts the vCenter Server installer.
- 6 Follow the prompts in the installation wizard to choose the installer language, agree to the end user patent and license agreements, enter your user name, organization name, and license key.

If you omit the license key, vCenter Server will be in evaluation mode, which allows you to use the full feature set for a 60-day evaluation period. After installation, you can enter the license key to convert vCenter Server to licensed mode.

- 7 Select the type of database to use.

Option	Action
<b>Install SQL Server 2008 Express instance (for small-scale deployments)</b>	Select this option if you used the bundled SQL Express database on the source machine.
<b>Use an existing supported database</b>	Select this option to use an existing non-bundled database. Select the DSN that was used for the database on the source machine, type the user name and password for the DSN, and click <b>Next</b> . If you specify a remote SQL Server database that uses Windows NT authentication, the database user and the logged-in user on the vCenter Server machine must be the same.

- 8 Select how to upgrade vCenter Agent and click **Next**.

Option	Description
<b>Automatic</b>	vCenter Agent is upgraded on all hosts in the vCenter Server inventory.
<b>Manual</b>	All hosts are disconnected from vCenter Server. To upgrade vCenter Agent, reconnect the host to vCenter Server. Select this option if one of the following situations: <ul style="list-style-type: none"> <li>■ You need to control the timing of vCenter Agent upgrades on specific hosts.</li> <li>■ The number of hosts in the vCenter Server inventory is large, and you anticipate that upgrading vCenter Agent on all hosts would negatively affect vCenter Server performance.</li> </ul>

vCenter Agent is installed on each host in the inventory to enable vCenter Server to manage the host. vCenter Agent must be upgraded when vCenter Server is upgraded.

- 9 Type the password for the vCenter Service user account, if the user account is specified.

By default, **Use SYSTEM Account** is selected.

- 10 Specify the fully qualified domain name (FQDN).

- 11 Either accept the default destination folders or click **Change** to select another location, and click **Next**.

The installation path cannot have commas (,) or periods (.).

**NOTE** To install the vCenter Server on a drive other than C:, verify that the C:\WINDOWS\Installer folder is large enough to accommodate the Microsoft Windows Installer .msi file. If the folder is not large enough, your vCenter Server installation might fail.

- 12 Specify the port numbers for vCenter Server or accept the default port numbers.

The port numbers displayed are those that were backed up from the source installation.

- 13 Specify the port numbers for Inventory Service.

- 14 Select the amount of memory to allocate to the vCenter JVM in Tomcat, according to the number of hosts in your environment.

You can adjust this setting after installation if the number of hosts in your environment changes.

- 15 In the Ready to Install the Program page, select **Select to bump up the ephemeral port value**.

This option increases the number of available ephemeral ports. If your vCenter Server manages hosts on which you will power on more than 2000 virtual machines simultaneously, selecting this option prevents the pool of available ephemeral ports from being exhausted.

- 16 Click **Install**.

The installation process might take several minutes.

- 17 After the installation process is completed, click **Finish**.

The data migration tool restores the backed up configuration data and starts the vCenter Server service.

- 18 Check the `\logs\restore.log` file in the `datamigration\logs` folder, and verify that no errors occurred during the restore process.
- vCenter Server and the Orchestrator client and server components are installed.
  - The configuration settings from your previous Orchestrator installation are imported.

### What to do next

Start the VMware vCenter Orchestrator Configuration service and log in to the Orchestrator configuration interface. If you migrated from vCenter Orchestrator 4.0, you must update the Orchestrator database.

If your Orchestrator database is local to the 32-bit Orchestrator server, it is inaccessible after the configuration backup. You must set up a new database and configure the database connection from the **Database** tab in the Orchestrator configuration interface.

For the detailed procedures, see

- [“Start the Orchestrator Configuration Service,”](#) on page 37
- [“Log In to the Orchestrator Configuration Interface,”](#) on page 38
- [“Configure the Database Connection,”](#) on page 49

## Uninstall Orchestrator

You can remove the Orchestrator client and server components from your system by using **Add or Remove Programs**.

### Prerequisites

- Save the Orchestrator configuration settings to a local file. For more details, see [“Export the Orchestrator Configuration,”](#) on page 29.
- Back up custom workflows and plug-ins.

### Procedure

- 1 From the Windows **Start** menu, select **Settings > Control Panel > Add or Remove Programs**.
- 2 Select **vCenter Orchestrator** and click **Remove**.
- 3 Click **Uninstall** in the Uninstall vCenter Orchestrator window.  
A message confirms that all items have been successfully removed.
- 4 Click **Done**.

Orchestrator is uninstalled from your system.

# Initial Configuration of the Orchestrator Server

# 5

The Orchestrator Web Configuration tool is installed silently with vCenter Server. You can use this tool to configure the components that are related to the Orchestrator engine, such as network, database, server certificate, and so on. The correct configuration of these components ensures the proper functioning of the applications running on the Orchestrator platform.

This chapter includes the following topics:

- [“Start the Orchestrator Configuration Service,”](#) on page 37
- [“Log In to the Orchestrator Configuration Interface,”](#) on page 38
- [“Change the Default Password,”](#) on page 39
- [“Configure the Orchestrator Configuration Interface for Remote Connection,”](#) on page 39
- [“Configure the Network Connection,”](#) on page 40
- [“Orchestrator Network Ports,”](#) on page 40
- [“Import the vCenter Server SSL Certificate,”](#) on page 42
- [“Configuring LDAP Settings,”](#) on page 42
- [“Configuring the Orchestrator Database Connection,”](#) on page 48
- [“Server Certificate,”](#) on page 51
- [“Configure the Default Plug-Ins,”](#) on page 54
- [“Import the vCenter Server License,”](#) on page 58
- [“Start the Orchestrator Server,”](#) on page 59

## Start the Orchestrator Configuration Service

If you have installed Orchestrator as a part of the vCenter Server installation, the Orchestrator Configuration service does not start by default. You must start it manually before you try to access the Orchestrator configuration interface.

If you installed Orchestrator standalone, the Orchestrator Configuration service is already started.

### Procedure

- 1 On the machine on which Orchestrator is installed, select **Start > Programs > Administrative Tools > Services**.
- 2 In the Services window, right-click **VMware vCenter Orchestrator Configuration** and select **Start**.

- 3 (Optional) Set up the service to start automatically on the next reboot.
  - a Right-click **VMware vCenter Orchestrator Configuration** and select **Properties**.
  - b In the VMware vCenter Orchestrator Configuration Properties (Local Computer) window, from the **Startup type** drop-down menu select **Automatic**.

The Orchestrator Configuration service is now running and Orchestrator configuration interface is available for use.

### What to do next

You can log in to the Orchestrator configuration interface and start the process of configuring Orchestrator.

## Log In to the Orchestrator Configuration Interface

To start the configuration process, you must access the Orchestrator configuration interface.

By default, you can access the Orchestrator configuration interface only on localhost. You can configure the Orchestrator configuration interface for remote connection.

### Prerequisites

Ensure that the VMware vCenter Orchestrator Configuration service is running.



**CAUTION** To avoid potential exploitation of the administrative credentials, change the nonsecure password when you first access the configuration interface. Retaining the default password might cause serious security issues in a production environment and is a common cause of data breach.

### Procedure

- 1 Start the Orchestrator configuration interface.
  - If you are logged in to the Orchestrator server machine as the user who installed Orchestrator, select **Start > Programs > VMware > vCenter Orchestrator Configuration**.
  - If you are logged in to the Orchestrator server machine as a different user than the user who installed Orchestrator, you cannot view the Orchestrator configuration shortcut in the **Start** menu. To access the configuration interface, go to `install_directory\Orchestrator\configuration` and double-click the `VMOConfiguration` shortcut.
  - Go to the following URL address in a Web browser:  
`http://localhost:8282`  
 8282 is the default HTTP access port reserved for the Web UI of Orchestrator configuration. To enable HTTPS connection through port 8283, you must configure Jetty to use SSL. For more details, see the *Jetty documentation*.
- 2 Log in with the default credentials.
  - User name: **vmware**.  
 You cannot change the **vmware** default user name.
  - Password: **vmware**.

When you log in to the Orchestrator configuration interface for the first time, you see the installation path, the Orchestrator version, and the server status in the **Information** tab. The status indicators of all tabs on the left display red triangles, which means that the components are not configured.

### What to do next

Change the default password.

## Change the Default Password

You must change the default password to avoid potential security issues.

### Prerequisites

Ensure that the VMware vCenter Orchestrator Configuration service is running.



**CAUTION** To avoid potential exploitation of the administrative credentials, change the nonsecure password when you first access the configuration interface. Retaining the default password might cause serious security issues in a production environment and is a common cause of data breach.

### Procedure

- 1 Log in to the Orchestrator configuration interface as **vmware**.
- 2 On the **General** tab, click **Change Password**.
- 3 In the **Current password** text box, enter **vmware**.
- 4 In the **New password** text box, enter the new password.
- 5 Reenter the new password to confirm it.
- 6 Click **Apply changes**.

## Configure the Orchestrator Configuration Interface for Remote Connection

By default, you can access the Orchestrator configuration interface only on **localhost**. You can configure the Orchestrator configuration interface for remote connection.

### Procedure

- 1 Log in as an administrator to the machine on which the Orchestrator server component is installed.
- 2 Navigate to the `jetty.xml` configuration file, and open it in a text editor.

Option	Action
<b>If you installed the standalone version of Orchestrator</b>	Go to <code>install_directory\VMware\Orchestrator\configuration\jetty\etc\jetty.xml</code> .
<b>If the vCenter Server installed Orchestrator</b>	Go to <code>install_directory\VMware\Infrastructure\Orchestrator\configuration\jetty\etc\jetty.xml</code> .

- 3 Find the following entry in the `jetty.xml` file.  

```
<SystemProperty name="jetty.host" default="localhost"/>
```
- 4 Replace **localhost** with **0.0.0.0**.
- 5 Restart the Orchestrator configuration service.
  - a Log in to the Orchestrator configuration interface as **vmware**.
  - b Click **Startup Options**.
  - c Click **Restart the vCO configuration server**.

You can access the Orchestrator configuration interface remotely.

## Configure the Network Connection

When you install Orchestrator, the IP address that the Orchestrator client interface uses to communicate to the server is not set automatically. To change this, you must configure the network settings used by Orchestrator.

### Prerequisites

Make sure that the network provides a fixed IP, which is obtained by using a properly configured DHCP server (using reservations) or by setting a static IP. The Orchestrator server requires that the IP address remains constant while it is running.

### Procedure

- 1 Log in to the Orchestrator configuration interface as **vmware**.
- 2 Click **Network**.
- 3 From the **IP address** drop-down menu, select the IP address to which you want to bind the Orchestrator server.

Orchestrator discovers the IP address of the machine on which the server is installed.

The corresponding DNS name appears. If no network name is found, the IP address appears in the **DNS name** text box. Use this IP address to log in to the Orchestrator client interface.

- 4 Set up the communication ports.

For more information about default ports, see [“Orchestrator Network Ports,”](#) on page 40.

- 5 Click **Apply changes**.

### What to do next

Click **SSL Certificate** to load the vCenter Server SSL certificate in Orchestrator.

## Orchestrator Network Ports

Orchestrator uses specific ports that allow communication with the other systems. Some of the communication ports you must set are a subset of the standard ports that the Orchestrator JBoss application server uses. The ports are set with a default value, but you can change these values at any time. When you make the changes, verify that all ports are free on your host and, if necessary, open these ports on required firewalls.

### Default Configuration Ports

To provide the Orchestrator service, you must set the default ports and configure your firewall to allow incoming TCP connections.

---

**NOTE** Other ports might be required if you are using custom plug-ins.

---

**Table 5-1.** VMware vCenter Orchestrator Default Configuration Ports

Port	Number	Protocol	Source	Target	Description
Lookup port	8230	TCP	Orchestrator client	Orchestrator server	The main port to communicate with the Orchestrator server (JNDI port). All other ports communicate with the Orchestrator client through this port. It is part of the JBoss application server infrastructure.
Command port	8240	TCP	Orchestrator client	Orchestrator server	The application communication port (RMI container port) used for loading the Orchestrator client remotely. It is part of the JBoss application server infrastructure.

**Table 5-1.** VMware vCenter Orchestrator Default Configuration Ports (Continued)

Port	Number	Protocol	Source	Target	Description
Messaging port	8250	TCP	Orchestrator client	Orchestrator server	The Java messaging port used for dispatching events. It is part of the JBoss application server infrastructure.
Data port	8244	TCP	Orchestrator client	Orchestrator server	The port used for accessing all Orchestrator data models, such as workflows and policies. It is part of the JBoss application server infrastructure.
HTTP server port	8280	TCP	End-user Web browser	Orchestrator server	The port used by the Orchestrator server to connect to the Web view front end through HTTP.
HTTPS server port	8281	TCP	End-user Web browser	Orchestrator server	The SSL secured HTTP protocol used to connect to the Web view front end and to communicate with the vCenter Server API.
Web configuration HTTP access port	8282	TCP	End-user Web browser	Orchestrator configuration	The access port for the Web UI of Orchestrator configuration.
Web configuration HTTPS access port	8283	TCP	End-user Web browser	Orchestrator configuration	The SSL access port for the Web UI of Orchestrator configuration. <b>NOTE</b> To enable the HTTPS connection, configure Jetty to use SSL. See <a href="#">Jetty Documentation, Configuring SSL</a> .

## External Communication Ports

You must configure your firewall to allow outgoing connections so that Orchestrator can communicate with external services.

**Table 5-2.** VMware vCenter Orchestrator External Communication Ports

Port	Number	Protocol	Source	Target	Description
LDAP	389	TCP	Orchestrator server	LDAP server	The lookup port of your LDAP Authentication server.
LDAP using SSL	636	TCP	Orchestrator server	LDAP server	The lookup port of your secure LDAP Authentication server.
LDAP using Global Catalog	3268	TCP	Orchestrator server	Global Catalog server	The port to which Microsoft Global Catalog server queries are directed.
SQL Server	1433	TCP	Orchestrator server	Microsoft SQL Server	The port used to communicate with the Microsoft SQL Server or SQL Server Express instances that are configured as the Orchestrator database.
Oracle	1521	TCP	Orchestrator server	Oracle DB Server	The port used to communicate with the Oracle Database Server that is configured as the Orchestrator database.
SMTP Server port	25	TCP	Orchestrator server	SMTP Server	The port used for email notifications.
vCenter Server API port	443	TCP	Orchestrator server	vCenter Server	The vCenter Server API communication port used by Orchestrator to obtain virtual infrastructure and virtual machine information from the orchestrated vCenter Server instances.

## Internal JBoss Ports

Internal JBoss Server ports do not need to be added to the firewall exceptions.

**Table 5-3.** Internal JBoss Server Ports

Port Number	Description
3455	RMI server registry invoker
3873	EJB3 and AOP remoting connector
4445	JBoss pooled invoker
4446	Remoting server service connector
8083	Dynamic class and resource loader

## Import the vCenter Server SSL Certificate

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.

### 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.

Option	Action
<b>Import from URL</b>	Specify the URL of the vCenter Server: <b><code>https://your_vcenter_server_IP_address</code></b>
<b>Import from file</b>	Obtain the vCenter Server certificate file. The file is usually available at the following locations: <ul style="list-style-type: none"> <li>■ C:\Documents and Settings\AllUsers\ApplicationData\VMware\VMware VirtualCenter\SSL\rui.crt</li> <li>■ /etc/vmware/ssl/rui.crt</li> </ul>

- 5 Click **Import**.

A message confirming that the import is successful appears.

- 6 Repeat the steps for each vCenter Server instance that you want to add to the Orchestrator server.

The imported certificate appears in the Imported SSL certificates list. On the **Network** tab, the red triangle changes to a green circle to indicate that the component is now configured correctly.

### What to do next

Each time you want to specify the use of an SSL connection to a vCenter Server instance, you must return to the **SSL Certificate** tab on the **Network** tab and import the corresponding vCenter Server SSL certificate.

## Configuring LDAP Settings

Orchestrator requires a connection to a working LDAP server on your infrastructure to manage user permissions.

If you are using secure LDAP over SSL, Windows 2003 or 2008, and AD, verify that the **LDAP Server Signing Requirements** group policy is disabled on the LDAP server.

- 1 [Generate the LDAP Connection URL](#) on page 43  
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.
- 2 [Import the LDAP Server SSL Certificate](#) on page 44  
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.
- 3 [Specify the Browsing Credentials](#) on page 45  
Orchestrator must read your LDAP structure to inherit its properties. You can specify the credentials that Orchestrator uses to connect to an LDAP server.
- 4 [Define the LDAP User and Group Lookup Paths](#) on page 46  
You can define the users and groups lookup information.
- 5 [Define the LDAP Search Options](#) on page 47  
You can customize the LDAP search queries and make searching in LDAP more effective.
- 6 [Common Active Directory LDAP Errors](#) on page 47  
When you encounter the LDAP: error code 49 error message and experience problems connecting to your LDAP authentication server, you can check which LDAP function is causing the problem.

## 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 44.

- 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 45.

## 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.

SSL capabilities are not installed as part of Microsoft Active Directory, eDirectory, and Sun Java Directory Server, and require more configuration. 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.

---

- 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

- Log in to the Orchestrator configuration interface as **vmware**.
- Click **LDAP**.
- 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.

- (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 it, you must select the **Dereference links** check box.

- (Optional) To filter the attributes that the search returns, select the **Filter attributes** check box.

Selecting this check box makes searching in LDAP faster. However, you might need to use some extra LDAP attributes for automation later.

- (Optional) Select the **Ignore referrals** check box to disable referral handling.

When you select the check box, the system does not display any referrals.

- In the **Host reachable timeout** text box, type a value in milliseconds.

This value determines the timeout period for the test checking the status of the destination host.

- Click **Apply changes**.

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

### What to do next

Configure the database. For more information, see [“Configuring the Orchestrator Database Connection,”](#) on page 48.

## Common Active Directory LDAP Errors

When you encounter the LDAP:error code 49 error message and experience problems connecting to your LDAP authentication server, you can check which LDAP function is causing the problem.

**Table 5-4.** Common Active Directory Authentication Errors

Error	Description
525	The user is not found.
52e	The user credentials are not valid.

**Table 5-4.** Common Active Directory Authentication Errors (Continued)

Error	Description
530	The user is not allowed to log in at this time.
531	The user is not allowed to log in to this workstation.
532	The password has expired.
533	This user account has been disabled.
701	This user account has expired.
773	The user must reset their password.
775	The user account has been locked.

## Configuring the Orchestrator Database Connection

The Orchestrator server requires a database in which to store data. To establish a connection with the database, you must configure the connection parameters.

Install a database and create a new database for Orchestrator. For more information, see [“Orchestrator Database Setup,”](#) on page 20. Configure the database for remote connection. For an example of configuring SQL Server Express for remote connection, see [“Configure SQL Server Express to Use with Orchestrator,”](#) on page 48.

### Configure SQL Server Express to Use with Orchestrator

You can use Microsoft SQL Server Express in small-scale environments.

Orchestrator can work with SQL Server Express when the deployment does not exceed 5 hosts and 50 virtual machines.

To use SQL Server Express with Orchestrator, you must configure the database to enable TCP/IP.

#### Procedure

- 1 Log in as an administrator to the machine on which SQL Server Express is installed.
- 2 Click **Start > All Programs > Microsoft SQL Server 2008 R2 > Configuration Tools > SQL Server Configuration Manager**.
- 3 Expand **SQL Server Network Configuration** in the list on the left.
- 4 Click **Protocols for SQLEXPRESS**.
- 5 Right-click **TCP/IP** and select **Enable**.
- 6 Right-click **TCP/IP** and select **Properties**.
- 7 Click the **IP Addresses** tab.
- 8 Under **IP1**, **IP2**, and **IPAll**, set the **TCP Port** value to **1433**.
- 9 Click **OK**.
- 10 Click **Server Services** on the left.
- 11 Restart the SQL Server.

#### What to do next

Configure the Orchestrator database connection parameters.

## 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. See [“Orchestrator Database Setup,”](#) on page 20.
- For a list of database connection parameters, see [“Database Connection Parameters,”](#) on page 50.
- 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 configuring the database connection and building 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 that you want Orchestrator server to use.

---

**NOTE** Orchestrator supports Oracle, SQL Server, and SQL Server Express.

---

- 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 or update the table structure for Orchestrator, install or update the database.

Option	Description
<b>Install the database</b>	Builds a new table structure for the Orchestrator database.
<b>Update the database</b>	Uses the database from your previous Orchestrator installation and updates the table structure.

After the database is populated, you can reset the database access rights to **db\_dataread** and **db\_datawrite**.

- 6 Click **Apply changes**.

---

**NOTE** If you change the Orchestrator database after configuring and installing the default plug-ins, you must click the **Troubleshooting** tab and force plug-in reinstallation by clicking the **Reset current version** link. This operation deletes the `install_directory\app-server\server\vm\plugins\VSOPuginInstallationVersion.xml` file, which holds the version of the plug-ins already installed, and forces plug-in reinstallation.

---

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.

## Example: Configure Orchestrator to Work with SQL Server Express by Using Windows Authentication Mode

If you want to use Orchestrator in small scale deployments for testing purposes, you might want to use SQL Server Express 2008 which you can install together with vCenter Server. After you create a new database for example *vco*, and enable it for remote connection, to configure the database connection perform the following steps:

- 1 Log in to the Orchestrator configuration interface as **vmware**.
- 2 Click the **Database** tab.
- 3 From the **Select the database type** drop-down menu, select **SQLServer**.
- 4 In the **User name** and **Password (if any)** text boxes, type your Windows credentials.
- 5 In the **Database host IP address or DNS name** text box, type the IP address of the machine on which Orchestrator and the database are installed.
- 6 In the **Port** text box, type the TCP/IP port of SQL Server, which usually is **1433**.
- 7 In the **Database name** text box, type the name of the SQL Server Express database you created, for example **vco**.
- 8 In the **Instance name (if any)** text box, type the name of the database instance.  
You can leave this field blank, if you have only one instance of SQL Server installed on the machine.
- 9 In the **Domain** text box either type the domain name of the machine on which Orchestrator and the database are installed, or type **localhost**.
- 10 Select **Use Windows authentication mode (NTLMv2)**.
- 11 Click **Apply**.
- 12 Build or update the database as necessary and click **Apply changes**.

You successfully configured Orchestrator to work with SQL Server Express by using Windows authentication mode.

## 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 5-5.** Database Connection Parameters

Connection Parameter	Description
User name	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 <b>db_owner</b> rights.
Password	The password for the user name you entered.
Database host IP address or DNS name	The database server IP address or DNS name.
Port	The database server port that allows communication to your database.
Database name	The full unique name of your database. The database name is specified by the <b>SERVICE_NAMES</b> parameter in the initialization parameter file.
Instance name (if any)	The name of the database instance that can be identified by the <b>INSTANCE_NAME</b> parameter in the database initialization parameter file.

**Table 5-5.** Database Connection Parameters (Continued)

Connection Parameter	Description
Domain (SQL Server only)	To use Windows authentication, specify the domain name of the SQL Server machine, for example <b>company.org</b> . To use SQL authentication, leave this text box blank.
Use Windows authentication mode (NTLMv2)	Select to send NTLMv2 responses when using Windows authentication. This option is valid only for SQL Server.

## Server Certificate

The server certificate is a form of digital identification that is used with HTTPS to authenticate Web applications. Issued for a particular server and containing information about the server's public key, the certificate allows you to sign all elements created in Orchestrator and guarantee authenticity. When the client receives an element from your server (typically this is a package), they verify your identity and decide whether to trust your signature.

- [Create a Self-Signed Server Certificate](#) on page 51  
Installing Orchestrator or deploying the Orchestrator requires that you create a certificate. You can create a self-signed certificate to guarantee encrypted communication and a signature for your packages. However, the recipient cannot be sure that the self-signed package that you are sending is in fact a package issued by your server and not a third party claiming to be you.
- [Obtain a Server Certificate Signed by a Certificate Authority](#) on page 52  
To provide recipients with an acceptable level of trust that the package was created by your server, certificates are typically signed by a certificate authority (CA). Certificate authorities guarantee that you are who you claim to be, and as a token of their verification, they sign your certificate with their own.
- [Import a Server Certificate](#) on page 52  
You can import a server certificate and use it with Orchestrator.
- [Export a Server Certificate](#) on page 53  
The server certificate private key is stored in the `vmw_keystore` table of the Orchestrator database. In case you lose or delete this key, or if you bind the Orchestrator server to a different database, the contents of the exported packages signed with this certificate become unavailable. To ensure that packages are decrypted on import, you must save this key to a local file.
- [Changing a Self-Signed Server Certificate](#) on page 53  
If you want to sign your packages with a server certificate different from the one you used for the initial Orchestrator configuration, you must export all your packages and change the Orchestrator database.

### Create a Self-Signed Server Certificate

Installing Orchestrator or deploying the Orchestrator requires that you create a certificate. You can create a self-signed certificate to guarantee encrypted communication and a signature for your packages. However, the recipient cannot be sure that the self-signed package that you are sending is in fact a package issued by your server and not a third party claiming to be you.

#### Procedure

- 1 Log in to the Orchestrator configuration interface as **vmware**.
- 2 Click **Server Certificate**.
- 3 Click **Create certificate database and self-signed server certificate**.
- 4 Type the relevant information.

- 5 From the drop-down menu, select a country.
- 6 Click **Create**.

Orchestrator generates a server certificate that is unique to your environment. The details about the certificate's public key appear in the Server Certificate window. The certificate's private key is stored in the `vmo_keystore` table of the Orchestrator database.

#### What to do next

For disaster recovery purposes, you can save the certificate private key to a local file.

## Obtain a Server Certificate Signed by a Certificate Authority

To provide recipients with an acceptable level of trust that the package was created by your server, certificates are typically signed by a certificate authority (CA). Certificate authorities guarantee that you are who you claim to be, and as a token of their verification, they sign your certificate with their own.

#### Procedure

- 1 Log in to the Orchestrator configuration interface as **vmware**.
- 2 Click **Server Certificate**.
- 3 Generate a Certificate Signing Request (CSR).
  - a Click **Export certificate signing request**.
  - b Save the `VS0certificate.csr` file in your file system when prompted.
- 4 Send the 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.
- 5 Click **Import certificate signing request signed by CA** and select the file sent by your CA.

Orchestrator uses the server certificate to perform the following tasks:

- Signs all packages before they are exported by attaching your certificate's public key to each one.
- Displays a user prompt after users import a package that contains elements signed by untrusted certificates.

#### What to do next

You can import this certificate on other servers.

## Import a Server Certificate

You can import a server certificate and use it with Orchestrator.

---

**IMPORTANT** You can import a certificate only if you have not created a self-signed certificate. If you have already created a certificate in the database, the option to import a certificate is not available.

---

#### Procedure

- 1 Log in to the Orchestrator configuration interface as **vmware**.
- 2 Click **Server Certificate**.
- 3 Click **Import certificate database**.
- 4 Browse to select the certificate file to import.

- 5 Type the password used to decrypt the content of the imported keystore database.

The details about the imported server certificate appear in the Server Certificate panel.

## Export a Server Certificate

The server certificate private key is stored in the `vmo_keystore` table of the Orchestrator database. In case you lose or delete this key, or if you bind the Orchestrator server to a different database, the contents of the exported packages signed with this certificate become unavailable. To ensure that packages are decrypted on import, you must save this key to a local file.

### Prerequisites

You must have created or imported a server certificate.

### Procedure

- 1 Log in to the Orchestrator configuration interface as **vmware**.
- 2 Click **Server Certificate**.
- 3 Click **Export certificate database**.
- 4 Type a password to encrypt the content of the exported keystore database.  
You must enter this password again when importing the file.
- 5 Click **Export**.
- 6 Save the `vmo-server.vmokeystore` file when prompted.

## Changing a Self-Signed Server Certificate

If you want to sign your packages with a server certificate different from the one you used for the initial Orchestrator configuration, you must export all your packages and change the Orchestrator database.

This workflow describes the process to change the self-signed certificate.

- 1 Export all your packages by using the Orchestrator client.
  - a Click the **Packages** view in the Orchestrator client.
  - b Right-click the package to export and select **Export package**.
  - c Browse to select a location to save the package to and click **Open**.
  - d Leave the **View content**, **Re-Packageable**, and **Edit element** options selected.



**CAUTION** Do not sign the package with your current certificate. You must not encrypt the package. When you delete the certificate database, the private key is lost and the contents of the exported package become unavailable.

---

- e (Optional) Deselect the **Export version history** check box if you do not want to export the version history.
  - f Click **Save**.
- 2 Create a new database and configure Orchestrator to work with it.  
For more information about setting up the Orchestrator database, see [“Configure the Database Connection,”](#) on page 49.
- 3 (Optional) Export the Orchestrator configuration to back up your configuration data in case you want to use the old database and the old SSL certificate.

You can export the Orchestrator configuration by using the Orchestrator configuration interface. For more information, see [“Export the Orchestrator Configuration,”](#) on page 29.

- 4 (Optional) Back up your database if you want to retain the old data.

The database that you bind Orchestrator to must not contain records in the `vmo_keystore` table.

- 5 Create a new self-signed certificate or import a server certificate signed by a certification authority.

You can create and import self-signed certificates by using the Orchestrator configuration interface. For more information, see [“Server Certificate,”](#) on page 51.

- 6 Configure your license settings.

You can configure the license settings from the Orchestrator configuration interface. For more information, see [“Import the vCenter Server License,”](#) on page 58.

- 7 Reinstall the default Orchestrator plug-ins.

- a On the Orchestrator configuration interface, click the **Troubleshooting** tab.
- b Click the **Reset current version** link.

- 8 Restart the Orchestrator server.

- a On the Orchestrator configuration interface, click the **Startup options**.
- b Click the **Restart service** link.

- 9 Reimport your packages.

- a Click the **Packages** view in the Orchestrator client.
- b From the drop-down menu, select **Import package**.
- c Browse to select the package to import and click **Open**.
- d Click **Import** or **Import and trust provider**.
- e Click **Import checked elements**.

The server certificate change is effective at the next package export.

## Configure the Default Plug-Ins

To deploy the set of default plug-ins when the Orchestrator server starts, the Orchestrator system must authenticate against the LDAP server. You can specify the administrative credentials that Orchestrator uses with plug-ins, and enable or disable plug-ins on the **Plug-ins** tab.

If you change the Orchestrator database after configuring and installing the default plug-ins, you must click the **Reset current version** link on the **Troubleshooting** tab. This operation deletes the `install_directory\app-server\server\vmo\plugins\_VSOPuginInstallationVersion.xml` file, which holds the version of the plug-ins already installed, and forces plug-in reinstallation.

### Prerequisites

Set up an LDAP server and configure the Orchestrator LDAP settings.

### Procedure

- 1 Log in to the Orchestrator configuration interface as **vmware**.
- 2 Click **Plug-ins**.

- 3 Type the credentials for a user who is a member of the Orchestrator Administration group that you specified on the **LDAP** tab.

When the Orchestrator server starts, the system uses these credentials to set up the plug-ins. The system checks the enabled plug-ins and performs any necessary internal installations such as package import, policy run, script launch, and so on.

- 4 (Optional) To disable a plug-in, deselect the check box next to it.

This action does not remove the plug-in file.

- 5 Click **Apply changes**.

On the **Plug-ins** tab, the red triangle changes to a green circle to indicate that the component is now configured correctly. The first time the server boots, it installs the selected plug-ins.

### What to do next

You can configure the settings for Mail, SSH, and vCenter Server plug-ins.

## Define the Default SMTP Connection

The Mail plug-in is installed with Orchestrator Server and is used for email notifications. The only option available for this plug-in is to use default values for new mail messages. You can set the default email account.

Avoid load balancers when configuring mail in Orchestrator. You might receive SMTP\_HOST\_UNREACHABLE error.

### Procedure

- 1 Log in to the Orchestrator configuration interface as **vmware**.
- 2 Click **Mail**.
- 3 Select the **Define default values** check box and fill in the required text boxes.

Text box	Description
<b>SMTP host</b>	Enter the IP address or domain name of your SMTP server.
<b>SMTP port</b>	Enter a port number to match your SMTP configuration. The default SMTP port is 25.
<b>User name</b>	Enter a valid email account. This is the email account Orchestrator uses to send emails.
<b>Password</b>	Enter the password associated with the user name.
<b>From name and address</b>	Enter the sender information to appear in all emails sent by Orchestrator.

- 4 Click **Apply changes**.

## Configure the SSH Plug-In

You can set up the SSH plug-in to ensure encrypted connections.

### Procedure

- 1 Log in to the Orchestrator configuration interface as **vmware**.
- 2 Click **SSH**.
- 3 Click **New connection**.

- 4 In the **Host name** text box, enter the host to access with SSH through Orchestrator.

---

**NOTE** The username and password are not required because Orchestrator uses the credentials of the currently logged-in user to run SSH commands. You must reproduce the accounts you want to work on SSH on target hosts from the LDAP server.

---

- 5 Click **Apply changes**.  
The host is added to the list of SSH connections.
- 6 (Optional) Configure an entry path on the server.
  - a Click **New root folder**.
  - b Enter the new path and click **Apply changes**.

The SSH host is available in the **Inventory** view of the Orchestrator client.

## Configure the vCenter Server 4.1 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. For more information, see [“Import the vCenter Server SSL Certificate,”](#) on page 42.

### Procedure

- 1 Log in to the Orchestrator configuration interface as **vmware**.
- 2 Click **vCenter Server 4.1**.
- 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 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.

- Specify the method you use to manage user access on the vCenter Server host.

Option	Action
<b>Share a unique session</b>	Select this option to allow Orchestrator to create only one connection to vCenter Server. Type the credentials of a user who is a vCenter Server administrator.
<b>Session per user</b>	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. <b>CAUTION</b> Each user who logs in to Orchestrator creates a new session to vCenter Server. This might rapidly use CPU, memory, and bandwidth.

- Click **Apply changes**.

The URL to the newly configured vCenter Server host is added to the list of defined hosts.

- Repeat [Step 3](#) through [Step 11](#) for each vCenter Server instance.

## Installing a New Plug-In

After you configure the default Orchestrator plug-ins, you might want to install a new plug-in.

All Orchestrator plug-ins are installed from the Orchestrator configuration interface. The allowed file extensions are `.vmoapp` and `.dar`. A `.vmoapp` file can contain a collection of several `.dar` files and can be installed as an application, while a `.dar` file contains all the resources associated with one plug-in.

You install `.vmoapp` files from the **General** tab of the Orchestrator configuration interface, and `.dar` files from the **Plug-ins** tab.

### Install a New DAR Plug-In

After you configure the default Orchestrator plug-ins you might want to install a new `.dar` plug-in.

#### Procedure

- Log in to the Orchestrator configuration interface as **vmware**.
- Click the **Plug-ins** tab.
- Click the magnifying glass icon under Install new plug-in.
- Browse to locate the `.dar` file, and click **Open**.
- Click **Upload and install**.

The installed plug-in file is stored in the `install_directory\app-server\server\vmo\plugins` folder.

### Install a New VMOAPP Plug-In

After you configure the default Orchestrator plug-ins, you might want to install a new `.vmoapp` plug-in.

#### Procedure

- Log in to the Orchestrator configuration interface as **vmware**.
- On the **General** tab, click **Install Application**.
- Click the magnifying glass icon.
- Browse to locate the `.vmoapp` file, and click **Open**.
- Click **Install**.

The tab for the plug-in appears in the Orchestrator configuration interface.

- 6 On the **Startup Options** tab, click **Restart service** to complete the plug-in installation.

You successfully installed the plug-in. Every time you install a `.vmoapp` plug-in, a validation is made on the server configuration. In most cases, you must perform additional configuration steps on a tab that the new application adds to the Orchestrator configuration interface.

## Import the vCenter Server License

To complete the configuration process for the Orchestrator server, you must import the vCenter Server license. The set of plug-ins delivered with Orchestrator does not require a license. If you add a plug-in that requires a license, you must import the license.

### Prerequisites

Import the SSL certificate for the licensed vCenter Server host. See [“Import the vCenter Server SSL Certificate,”](#) on page 42.

### Procedure

- 1 Log in to the Orchestrator configuration interface as **vmware**.
- 2 Click **Licenses**.
- 3 On the **vCenter Server License** tab, specify the details about the vCenter Server host on which Orchestrator must verify the license key.
  - a In the **Host** text box, type the IP address or the DNS name of the vCenter Server host.
  - b In the **Port** text box, leave the default value, **443**.
  - c (Optional) Select the **Secure channel** check box to establish a secure connection to the vCenter Server host.
  - d In the **Path** text box, use the default value, `/sdk`.  
This is the location of the SDK that you use to connect to your vCenter Server instance.
  - e In the **User name** and **Password** text boxes, type the credentials that Orchestrator must use to establish the connection to vCenter Server.  
The user you select must be a valid user with administrative privileges on your vCenter Server, preferably at the top of the vSphere tree structure.
- 4 (Optional) To view details, click **License details**.
- 5 (Optional) If the version of your vCenter Server is earlier than version 4.0, you must add the license key manually.
  - a Click the **Add vCenter Server license manually** radio button.
  - b In the **Serial number** text box, type your vCenter Server license key.
- 6 Click **Apply changes**.
- 7 (Optional) To view details, click the name of the imported license.
- 8 Start the Orchestrator server.

The Orchestrator server is now configured correctly.

## Access Rights to Orchestrator Server

The type of vCenter Server license you apply in the Orchestrator configuration interface determines whether you get read-only or full access to the Orchestrator server capabilities.

**Table 5-6.** Orchestrator Server Modes

vCenter Server License Edition	vCenter Orchestrator Mode	Description
Standard	Server	You are granted full read and write privileges to all Orchestrator elements. You can run and edit workflows.
Foundation	Player	You are granted read privileges on all Orchestrator elements. You can run workflows but you cannot edit them.
Essentials	Player	You are granted read privileges on all Orchestrator elements. You can run workflows but you cannot edit them.
Evaluation	Server	You are granted full read and write privileges to all Orchestrator elements. You can run and edit workflows.

**NOTE** All predefined workflows are locked as read-only by design. To edit a standard workflow, you must duplicate the workflow and make changes to the duplicated workflow.

## Start the Orchestrator Server

You can install the Orchestrator server as a service from the **Startup Options** tab of the Orchestrator configuration interface. When you do this, you can start, stop, and restart the service from the Orchestrator configuration interface. This process is reversible, as you always have the choice of using the **Uninstall vCO server from service** option.

### Prerequisites

- If you installed Orchestrator silently with vCenter Server, verify that your system has at least 4GB of RAM and that the database is running on a dedicated server. The Orchestrator server might not start if your system does not meet this requirement.
- If you installed Orchestrator standalone, verify that your system has at least 2GB of RAM. The Orchestrator server might not start if your system does not meet this requirement.
- All of the status indicators must display a green circle. You cannot start the Orchestrator server if any of the components is not configured properly.

### Procedure

- 1 Log in to the Orchestrator configuration interface as **vmware**.
- 2 Click **Startup Options**.
- 3 Click **Install vCO server as service**.

The Orchestrator server is installed as a Windows service.

- 4 Click **Start service**.

The Orchestrator server status appears as **Service is starting**. The first boot can take 5-10 minutes because it is installing the Orchestrator plug-ins content in the database tables.

A message states that the service is started successfully. The Orchestrator server status appears at the bottom of each configuration tab, and is one of the following:

- Running
- Not available
- Stopped

To see the Orchestrator server status, update the page by clicking the **Refresh** link.

**What to do next**

You can save and export the Orchestrator configuration file so that it can be imported later if needed. See [“Export the Orchestrator Configuration,”](#) on page 29.

## Further Configuration Options

---

You can use the Orchestrator configuration interface to change the default Orchestrator behavior.

This chapter includes the following topics:

- [“Revert to the Default Password for Orchestrator Configuration,”](#) on page 61
- [“Change the Default Configuration Ports on the Orchestrator Client Side,”](#) on page 62
- [“Uninstall a Plug-In,”](#) on page 63
- [“Activate the Service Watchdog Utility,”](#) on page 63
- [“Unwanted Server Restarts,”](#) on page 64
- [“Export the Orchestrator Configuration,”](#) on page 64
- [“Import the Orchestrator Configuration,”](#) on page 66
- [“Configure the Maximum Number of Events and Runs,”](#) on page 66
- [“Import the Plug-In Licenses,”](#) on page 67
- [“Changing SSL Certificates,”](#) on page 67
- [“Define the Server Log Level,”](#) on page 69

### Revert to the Default Password for Orchestrator Configuration

If the default password for the Orchestrator configuration interface is changed, you cannot retrieve it because Orchestrator uses encryption to encode passwords. You can revert to the default password **vmware** if the current password is not known.

#### Procedure

- 1 Navigate to the following folder on the Orchestrator server system.

Option	Action
<b>If you installed Orchestrator with the vCenter Server installer</b>	Go to <i>install_directory</i> \VMware\Infrastructure\Orchestrator\configuration\jetty\etc.
<b>If you installed the standalone version of Orchestrator</b>	Go to <i>install_directory</i> \VMware\Orchestrator\configuration\jetty\etc.

- 2 Open the `password.properties` file in a text editor.
- 3 Delete the content of the file.

- 4 Add the following line to the `password.properties` file.  
`vmware=92963abd36c896b93a36b8e296ff3387`
- 5 Save the `password.properties` file.
- 6 Restart the vCenter Orchestrator Configuration service.

You can log in to the Orchestrator configuration interface with the default credentials.

- User name: **vmware**
- Password: **vmware**

## Password Encryption and Hashing Mechanism

Orchestrator utilizes PBE with MD5 and DES encryption mechanism to encode the stored passwords used to connect to the database, LDAP, and Orchestrator servers.

**Table 6-1.** Encryption and Hashing Algorithms in Orchestrator

Algorithm	Description
Password Based Encryption (part of Java 2 SDK 1.4)	Generates an encryption key from a password. PBE stores and checks the hash value of the password. For more information, see the <i>Java Cryptography Extension Reference Guide</i> on java.sun.com.
Message Digest 5 algorithm	Generates a 128-bit cryptographic message digest value, usually expressed as a 32 digit hexadecimal number.
Data Encryption Standard	Applies a 56-bit key to each 64-bit block of data.

## Change the Default Configuration Ports on the Orchestrator Client Side

If you change the default network ports in the Orchestrator configuration interface, your changes are applied only on the Orchestrator server side. To connect to the server with the client, you must change the configuration of all Orchestrator client instances or connect to the server by using your Orchestrator server DNS name or IP address followed by the new lookup port number.

The main port to communicate with the Orchestrator server is the lookup port. The Orchestrator client discovers all other ports through this port. If you change the default lookup port value in the Orchestrator configuration interface after you install the Orchestrator client instances, you can add a `vmo.properties` configuration file for each Orchestrator client instance and define the new lookup port by adding the `ch.dunes.net.jboss-server.port` system property.

### Procedure

- 1 Log in as an administrator on the machine where the Orchestrator client is installed.
- 2 Navigate to the `apps` folder.

Option	Action
<b>If you installed Orchestrator with the vCenter Server installer</b>	Go to <code>install_directory\VMware\Infrastructure\Orchestrator\apps</code> .
<b>If you installed the standalone version of Orchestrator</b>	Go to <code>install_directory\VMware\Orchestrator\apps</code> .

- 3 In a text editor, create a file that contains the lookup port value.  
`ch.dunes.net.jboss-server.port=new_lookup_port_number`
- 4 Save the file as `vmo.properties`.

- 5 Repeat the procedure for every Orchestrator client instance.

You can connect to the Orchestrator server by using the Orchestrator client without adding the lookup port number to the Orchestrator server DNS name or IP address.

## Uninstall a Plug-In

You can disable an Orchestrator plug-in from the **Plug-ins** tab, but this does not remove the plug-in file from the file system. To remove the plug-in file, you must log in to the machine on which the Orchestrator server is installed and remove the plug-in file manually.

### Procedure

- 1 Log in as an administrator to the machine on which the Orchestrator server is installed.
- 2 Navigate to the Orchestrator installation folder.

Option	Action
<b>If you installed Orchestrator with the vCenter Server installer</b>	Go to <code>install_directory\VMware\Infrastructure\Orchestrator\app-server\server\vm\plugins</code> .
<b>If you installed the standalone version of Orchestrator</b>	Go to <code>install_directory\VMware\Orchestrator\app-server\server\vm\plugins</code> .

- 3 Delete the .dar archive that contains the plug-in to remove.
- 4 Restart the vCenter Orchestrator Configuration service.  
The plug-in is removed from the Orchestrator configuration interface.
- 5 Log in to the Orchestrator client.
- 6 In the Orchestrator client, click the **Packages** view.
- 7 Right-click the package to delete, and select **Delete element with content**.

---

**NOTE** Orchestrator elements that are locked in the read-only state, for example workflows in the standard library, are not deleted.

---

You removed all custom workflows and actions, policies, Web views, configurations, settings, and resources that the plug-in contains.

## Activate the Service Watchdog Utility

Orchestrator provides a watchdog utility that checks whether the Orchestrator server service is running. The utility pings the Orchestrator server service periodically, and restarts it if a certain timeout period is exceeded.

By default, the watchdog utility is deactivated.

You can activate the service watchdog utility by setting the timeout period for the service's response to the ping from the utility. You can set the timeout period for the response from the Orchestrator server service in the `wrapper.conf` configuration file. The `wrapper.conf` file defines the wrapping of the Orchestrator server in the host system.

### Prerequisites

The Orchestrator server must be running as a Windows service.

### Procedure

- 1 Log in as an administrator to the machine on which the Orchestrator server is installed.

- 2 Navigate to the `wrapper.conf` configuration file and open the file in a text editor.

The wrapper configuration file is in the following location:

```
install_directory/app-server/bin/wrapper.conf
```

- 3 Locate the `-wrapper.ping.timeout` parameter in the `wrapper.conf` file, or add it to the file if it does not exist.

- 4 Set the number of seconds to allow between a ping from the watchdog utility and the response from the service.

The default timeout is 0 seconds, which means that the utility is deactivated.

For example, you can increase the timeout period to 30 seconds by setting the parameter as follows:

```
-wrapper.ping.timeout=30
```

- 5 Save and close the `wrapper.conf` file.
- 6 Log in to the Orchestrator configuration interface as **vmware**.
- 7 On the **Startup Options** tab, click **Restart Service** to restart the Orchestrator server.

You activated the Orchestrator watchdog utility by setting the timeout.

## Unwanted Server Restarts

You might experience unwanted server restarts if you have activated the service watchdog utility.

### Problem

In certain circumstances, if the response time exceeds the watchdog timeout period, the watchdog utility can falsely detect a JVM error, which causes a server restart.

### Cause

The problem occurs when the Orchestrator server is running with a heavy load, for example if you have connected Orchestrator to many vCenter Server instances that are running many virtual machines, or if the server is performing swapping.

### Solution

If you experience this behavior, extend the watchdog timeout period by increasing the timeout parameter in the `wrapper.conf` configuration file. If the problem still persists, deactivate the watchdog utility by setting the timeout parameter back to zero (0). See [“Activate the Service Watchdog Utility,”](#) on page 63.

## Export the Orchestrator Configuration

The Orchestrator configuration interface provides a mechanism to export the Orchestrator configuration settings to a local file. This mechanism allows you to take a snapshot of your system configuration at any moment and import this configuration into a new Orchestrator instance.

You should export and save your configuration settings on a regular basis, especially when making modifications, performing maintenance, or upgrading the system.

For a list of exported configuration settings, see [“Orchestrator Configuration Files,”](#) on page 65.

### Procedure

- 1 Log in to the Orchestrator configuration interface as **vmware**.
- 2 On the **General** tab, click **Export Configuration**.

- 3 (Optional) Type a password to protect the configuration file.  
Use the same password when you import the configuration.
- 4 Click **Export**.
- 5 Click **Save** when prompted.

Orchestrator creates a `vmo_config_dateReference.vmoconfig` file which you can use to clone or to restore the system.

## Orchestrator Configuration Files

When you export the system configuration, a `vmo_config_dateReference.vmoconfig` file is created locally. It contains all the Orchestrator configuration data.

**NOTE** Some of the configuration files that are created during the export are empty. For example, the server configuration data is not exported because the startup options for the Orchestrator server are individual for each machine where the Orchestrator server is installed. These empty files must be reconfigured, even when a working configuration was previously imported.

**Table 6-2.** Settings Not Saved During Configuration Export

Setting	Description
Certificate	Certificates are not exported. Most certificates are stored in the Orchestrator database. However, the vCenter Server certificate is not stored in the database. You must store it in a separate location, or import it again when you import an Orchestrator configuration.
Licenses	Manually imported licenses are not exported. They are stored in the Orchestrator database.
Server	The server configuration is reset to Unknown. You must install the Orchestrator server as a Windows service again.

**Table 6-3.** Settings Saved During Configuration Export

Setting	Description
General	The maximum number of completed events and workflows recorded, and the Web view development and configuration.
Network	The IP binding address and the TCP ports used by the different elements of the Orchestrator server.
Database	The database configuration.
LDAP	The LDAP server configuration.
Log	The log settings information.
Plug-ins	The list of disabled plug-ins and the account name.
Mail plug-in	The SMTP host, SMTP port, user name, password, sender's name, sender's address.
vCenter Server plug-in	The vCenter Server plug-in configuration.
License	The details about the vCenter Server host on which Orchestrator verifies the license key.

## Import the Orchestrator Configuration

You can restore the previously exported system configuration if a system failure occurs or when you reinstall Orchestrator.

### Procedure

- 1 Log in to the Orchestrator configuration interface as **vmware**.
- 2 On the **General** tab, click **Import Configuration**.
- 3 Type the password you used when exporting the configuration.  
This step is not necessary, if you have not specified a password.
- 4 Browse to select the `.vmoconfig` file you exported from your previous installation.
- 5 Click **Import**.

A message states that the configuration is successfully imported. The new system replicates the old configuration completely.

## Configure the Maximum Number of Events and Runs

You can define the maximum number of events stored in the Orchestrator database and the maximum number of workflow runs.

Each event corresponds to a change in the state of a workflow or policy and is stored in the database. When the maximum number of events set for a workflow or policy is reached, the database deletes the oldest event to store the new event.

Each time you run a workflow, a workflow token is created in the database. This token contains all parameters related to the running of the workflow. For example, if you run a workflow three times, three workflow tokens are created. The three tokens appear in the Orchestrator client below the workflow.

### Procedure

- 1 Log in to the Orchestrator configuration interface as **vmware**.
- 2 On the **General** tab, click **Advanced Configuration**.
- 3 Fill in the **Max number of events** text box.  
To track every change in your infrastructure, type **0**. This means that the server never rolls over, but it might become unavailable. Database administrators must periodically clean the server and archive events.
- 4 Fill in the **Max number of runs** text box.  
After you reach the maximum number of runs, the rollover process starts. If you do not want the rollover process to start, type **0** in this text box. If you type **0**, your database continues to extend.
- 5 (Optional) To set the default login credentials, fill in the **User name for automatic Web login** and **Password for automatic Web login** text boxes.  
This feature allows you to generate URLs that enable you to run, answer, schedule, or monitor a workflow without having to specify your credentials. Use your default operator credentials for these text boxes.
- 6 Fill in the **Web view directory** text box.  
This is the root folder from which development Web views are loaded. Files for each Web view must be in a separate subfolder, and the name of this subfolder must be the same as the URL folder defined in the client.

- 7 (Optional) To put the server in Web view development mode, select the **Enable Web view development** check box.

In this mode, all elements in the Web view are loaded from the specified Web view directory and not from the Web view content itself. See *Developing with VMware vCenter Orchestrator*.

- 8 Click **Apply changes**.

## Import the Plug-In Licenses

The set of plug-ins that Orchestrator includes does not require a license. If you add a plug-in that requires a license, you must import it in the Orchestrator configuration interface.

### Procedure

- 1 Log in to the Orchestrator configuration interface as **vmware**.
- 2 Click **Licenses**.
- 3 On the **Licenses** tab, click **Plug-in Licenses**.
- 4 In the **Serial number** text box, type your plug-in license key.
- 5 Click **Apply changes**.

### What to do next

To view details, click the name of the imported license.

## Changing SSL Certificates

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

### 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.

```
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.

```
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.
 

```
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).
 

```
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 Web Views SSL Certificate

Orchestrator provides an SSL certificate that controls user access to Web views. You can configure Orchestrator to use a different SSL certificate to control access to Web views, for example if your company security policy requires you to use their SSL certificates.

### Prerequisites

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

### Procedure

- 1 Open the following Orchestrator application server configuration file in a text editor.

Option	Action
<b>If you installed the standalone version of Orchestrator</b>	Go to <i>install_directory\VMware\Orchestrator\app-server\server\vm\deploy\jboss-deploy-tomcat\jbossweb-tomcat55.sar\server.xml</i> .
<b>If the vCenter Server installed Orchestrator</b>	Go to <i>install_directory\VMware\Infrastructure\Orchestrator\app-server\server\vm\deploy\jboss-deploy-tomcat\jbossweb-tomcat55.sar\server.xml</i> .

- 2 Find the following entry at line 44 in the `server.xml` file.

```
<!-- Define a SSL HTTP/1.1 Connector on port ${ch.dunes.https-server.port} -->
<Connector address="${jboss.bind.address}" protocol="HTTP/1.1" SSLEnabled="true"
clientAuth="false" emptySessionPath="true"
keystoreFile="${java.home}/lib/security/jssecacerts"
keystorePass="dunesdunes"
maxHttpHeaderSize="8192" maxThreads="100"
port="${ch.dunes.https-server.port}" scheme="https" secure="true"
sslProtocol="TLS" strategy="ms" />
```

- 3 Change the `keystoreFile` and `keystorePass` attributes to refer to the `.keystore` file and the password you created when you ran the `keytool` utility.

```
keystoreFile="/PathToKeystore/.keystore"
keystorePass="NewKeystorePassword"
```

The `keystoreFile` attribute should contain slashes as directory separators.

- 4 Save the `server.xml` file and restart the Orchestrator server.

You changed the SSL certificate that the Orchestrator server uses to control access to Web views.

## Change the SSL Certificate for the Orchestrator Client

By default, the Orchestrator server uses the predefined SSL certificate while communicating remotely with the Orchestrator client. You can change the SSL certificate for the Orchestrator client, for example if your company security policy requires you to use its SSL certificates.

### Prerequisites

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

### Procedure

- 1 Open the following Orchestrator application server service file in a text editor.

Option	Action
<b>If you installed the standalone version of Orchestrator</b>	Go to <i>install_directory\VMware\Orchestrator\app-server\server\vmo\conf\jboss-service.xml</i> .
<b>If the vCenter Server installed Orchestrator</b>	Go to <i>install_directory\VMware\Infrastructure\Orchestrator\app-server\server\vmo\conf\jboss-service.xml</i> .

- 2 Find the following entry at line 359 in the *jboss-service.xml* file.

```
<!-- The SSL domain setup -->
<mbean code="org.jboss.security.plugins.JaasSecurityDomain"
name="Security:name=JaasSecurityDomain,domain=dunes">
  <constructor>
    <arg type="java.lang.String" value="dunes"/>
  </constructor>
  <attribute name="KeyStoreURL">${java.home}/lib/security/jssecacerts</attribute>
  <attribute name="KeyStorePass">dunesdunes</attribute>
</mbean>
```

- 3 Change the *keystoreURL* and *keystorePass* attributes to refer to the path to the *.keystore* file and the password you created when you ran the *keytool* utility.

```
keystoreURL="/PathToKeystore/.keystore"
keystorePass="NewKeystorePassword"
```

The *keystoreURL* attribute is a URL and must contain slashes as directory separators.

- 4 Save the *jboss-service.xml* file and restart the Orchestrator server.

The Orchestrator client authenticates the Orchestrator server by using the SSL certificate you changed.

## Define the Server Log Level

In the Orchestrator configuration interface, you can set the level of server log that you require. The default server log level is INFO. Changing the log level affects any new messages that the server writes to the server log and the number of active connections to the database.



**CAUTION** Only set the log level to DEBUG or ALL to debug a problem. Do not use this setting in a production environment because it can seriously impair performance.

### Procedure

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

- 3 Select an option from the **Log level** drop-down menu.

Option	Description
FATAL	Only fatal errors are written to the log file.
ERROR	Errors and fatal errors are written to the log file.
WARN	Warnings, errors, and fatal errors are written to the log file.
INFO	Information, warnings, errors, and fatal errors are written to the log file.
DEBUG	Debug information, information messages, warnings, errors, and fatal errors are written to the log file.
ALL	Events are not filtered. All events are written to the log file.
OFF	No entries are written to the log file and no log updates are made.

---

**NOTE** The log contains messages of the selected level and all higher levels. If you select the **INFO** level, all **INFO** messages and higher-level messages (**INFO**, **WARN**, **ERROR**, and **FATAL**) are written to the log file.

---

- 4 Click **Apply changes**.
- 5 (Optional) Click the **Generate log report** link to export the log files.

This operation creates a ZIP archive of all log files.

The new log level is applied to any new messages that the server generates, without restarting the server. The logs are stored in *install\_directory*\app-server\server\vmo\log\.

## Where to Go From Here

---

When you have installed and configured vCenter Orchestrator, you can use Orchestrator to automate frequently repeated processes related to the management of the virtual environment.

- Log in to the Orchestrator client, run, and schedule workflows on the vCenter Server inventory objects or other objects that Orchestrator accesses through its plug-ins.
- Publish the weboperator Web view and provide browser access to Orchestrator workflows to users and user groups.
- Set up the user permissions on Orchestrator objects.
- Duplicate and modify the standard Orchestrator workflows and write your own actions and workflows to automate operations in vCenter Server.
- Develop plug-ins, Web services, and Web views to extend the Orchestrator platform.

For information about features and instructions about using and maintaining Orchestrator, see *Administering VMware vCenter Orchestrator*.

For guidance with advanced development tasks and extending the Orchestrator platform, see *Developing with VMware vCenter Orchestrator*.



# Index

## A

audience 7  
availability 19

## C

certificate database 53  
changing the Orchestrator Lookup port 62  
check-pointing 11  
configuration  
  config files 65  
  database connection 48–50  
  default plug-ins 54  
  export configuration settings 29, 64  
  import configuration settings 31, 66  
  LDAP settings 46  
  network connection 40  
configuration maximums 19

## D

data migration tool  
  back up customized elements 33  
  export configuration settings 32  
  import configuration settings 34  
data migration 31  
database  
  connection parameters 49, 50  
  installation 20  
  Oracle 20  
  server size 20  
  setup 20  
  SQL Server 20  
  SQL Server Express 20  
default password 61  
default ports  
  command port 40  
  data port 40  
  HTTP port 40  
  HTTPS port 40  
  JBoss server ports 40  
  LDAP port 40  
  LDAP with Global Catalog 40  
  LDAP with SSL 40  
  lookup port 40  
  messaging port 40  
  Oracle port 40

SMTP port 40  
SQL Server port 40  
vCenter API port 40  
Web configuration HTTP access port 40  
Web configuration HTTPS access port 40

dereference links 47  
DES 62  
download the vCenter Server installer 21

## E

encryption 62  
events 66

## F

filter attributes 47  
further configuration options 61

## H

hashing 62

## I

i18n support 16  
ignore referrals 47  
install  
  .dar plug-in 57  
  .vmoapp plug-in 57  
installing, plug-in 57  
installing Orchestrator  
  vCenter Orchestrator client installers 25  
  vCenter Orchestrator standalone installer 24, 30  
  vCenter Server installer 22  
internationalization 16  
IPv4 22  
IPv6 22

## L

LDAP  
  browsing credentials 45  
  connection URL 43  
  LDAP Server Signing Requirements 44  
  lookup paths 46  
  SSL certificate 44  
LDAP errors  
  525 47  
  52e 47

- 530 **47**
- 531 **47**
- 532 **47**
- 533 **47**
- 701 **47**
- 773 **47**
- 775 **47**
- license
  - importing plug-in licenses **67**
  - importing vCenter Server license **58**
  - Orchestrator server access rights **59**
- load balancing **55**
- login **38**
  
- M**
- MD5 **62**
  
- N**
- non-ASCII characters **16, 24, 30, 49**
  
- O**
- Orchestrator architecture **13**
- Orchestrator client, change the SSL certificate **69**
- Orchestrator configuration interface, remote connection **39**
- Orchestrator installed on a 64-bit machine **29**
- Orchestrator overview **11**
  
- P**
- password **39**
- PBE **62**
- persistence **11**
- plug-ins, removing a plug-in **63**
- plug-ins configuration
  - Mail plug-in **55**
  - SSH plug-in **55**
  - vCenter Server plug-in **56**
- policy engine **11**
  
- R**
- runs **66**
  
- S**
- scalability **19**
- scripting engine **11**
- security **11**
- server certificate
  - CA-signed **51, 52**
  - exporting **51, 53**
  - importing **52**
  - removing **53**
  - self-signed **51**
- server log
  - exporting **69**
  - log level **69**
- service watchdog utility
  - timeout parameter **63**
  - troubleshooting server restarts **64**
- services
  - starting **37, 59**
  - VMware vCenter Orchestrator Configuration **37**
  - VMware vCenter Orchestrator Server **59**
- setup guidelines
  - directory services **20**
  - LDAP server **20**
  - vCenter Server **19**
- SMTP connection **55**
- SQL Express, configuring SQL Express **48**
- SSL certificate **42, 67**
- SSL certificates **67**
- system requirements
  - directory services **15**
  - hardware **15**
  - operating systems **15**
  - supported browsers **16**
  - supported databases **16**
  
- T**
- timeouts **47**
  
- U**
- uninstalling **30, 36**
- updated information **9**
- upgrading Orchestrator **21**
- upgrading Orchestrator 4.1 standalone **28**
- upgrading vCenter Server to upgrade Orchestrator **25**
- user roles **12**
  
- V**
- vCenter Server, downloading the installer **21**
- versioning **11**
- VMware vCenter Orchestrator Server, installing as Windows service **59**
  
- W**
- watchdog utility **63**
- Web views, change SSL certificate **68**
- what to do next **71**
- workflow engine **11**