Operations Orchestration

Software Version: 10.80

Windows and Linux

Install

Document Release Date: September 2017

Software Release Date: September 2017

Hewlett Packard Enterprise

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

Documentation Updates

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com/.

This site requires that you register for an HP Passport and to sign in. To register for an HP Passport ID, click **Register** on the HPE Software Support site or click **Create an Account** on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HPE sales representative for details.

Contents

Install

This section describes how to install OO Central, RAS, and Studio.

Before starting the installation:

- See the *System Requirement* section in *HCM Documentation* to verify that your system meets the minimum system requirements.
- Make sure that the person running the installation has Administrator privileges, in order to avoid UAC (user access control) errors. If you are not sure about your UAC settings, you can also right-click on the installer and choose to run it as an Administrator.

If you are connecting to a database with an existing schema, which Central already ran on, make sure that you use the same encryption key (**central/var/security/encryption_repository**) as the previous Central. Otherwise, Central will not start, and will show an exception message in the **wrapper.log** file ("bad padding"). This is because there is no way to decrypt the already-encrypted data with the new encryption key. If this problem occurs, see "Backing Up Operations Orchestration" in the Operations Orchestration*Administration Guide*.

To prevent this problem from occurring, when you install Central, select the **Do not start Central server after installation** check box in the **Connectivity** step of the installation wizard, or use the corresponding property if you're installing silently. Then, perform the task described in "Backing Up Operations Orchestration > Recovery" in the *Operations Orchestration Administration Guide*.

> **Note:** For more information about basic Operations Orchestration concepts, see the Operations Orchestration > Concepts Guide .

Deployment Architecture

Operations Orchestration Components

Operations Orchestration Studio is a standalone authoring program used for creating, modifying, and testing flows.

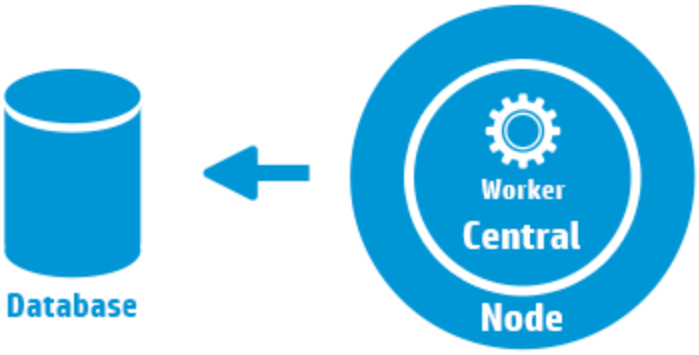
Operations Orchestration Central is the run time environment of Operations Orchestration. It is used for running flows, monitoring the various runs, and generating reports.

An **RAS** is a remote action server, containing a worker and a remote protocol for connecting with Central.

For additional information on Operations Orchestration components, see the *Operations Orchestration Concepts Guide*.

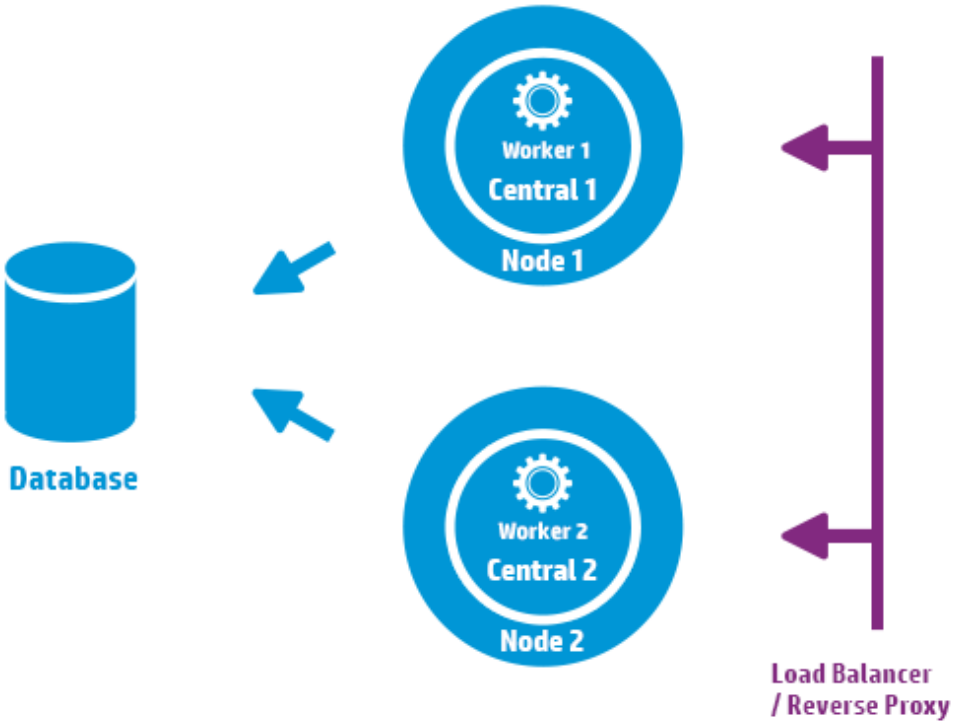
Simple Deployment

The basic Operations Orchestration deployment consist of a single Central instance, as shown in the image below.



Simple Cluster

In order to prevent the Central being the single point of failure, it is recommended to have a high-availability deployment. You can set a cluster of multiple Central nodes, the simplest of which contains two Central nodes connected to the same database schema. As shown in the image below, a load balancer can be set before the Central cluster to expose a single URL to the end users. Exposing a single URL can also be done with DNS load balancing.



The load balancer/reverse proxy should redirect to the Centrals that use ports 8443 and 8080, if the default values were chosen during installation. For more information, see the *Operations Orchestration* *"Support Matrix" on page 12*.

Load Balancer Requirements

We recommend to configure the load balancer with two separate virtual IPs for the user interface and for RASes:

- For the Operations Orchestration user interface and customer portals, the virtual IP should use a **sticky session** policy. The sticky session ensures that all subsequent requests will be sent to the server that handled the first login request. This means that users will only need to log in to the Operations Orchestration interface once.
- For RASes, the virtual IP should use a **round robin** policy, to distribute the load across the different servers.

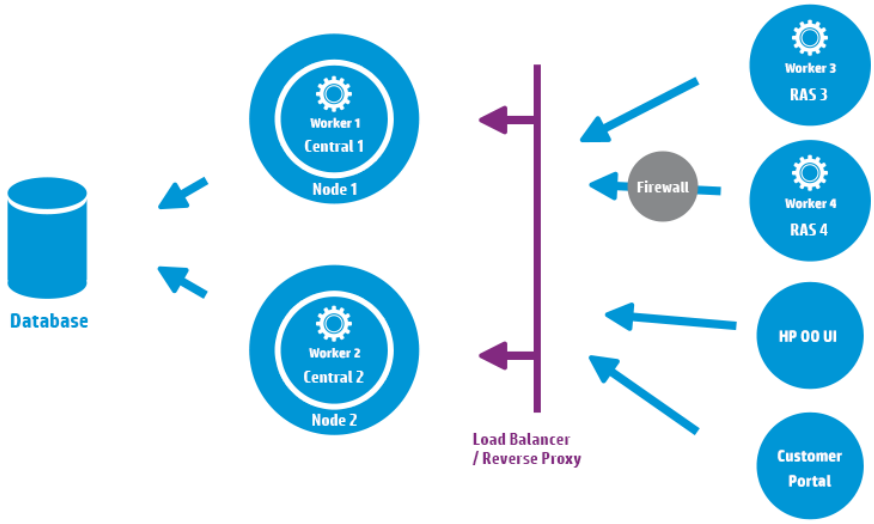
> **Note:** If you have a different configuration that satisfies these requirements, it is okay to use it. For example, if you have a load balancer that supports JSESSION, you can use the JSESSIONID parameter to set up a single virtual IP with a sticky session policy for all sources. Since RAS requests are stateless (no JSESSIONID), this will provide a round robin policy for RASes.

Central uses the following URL to check which server is live: HTTP://<IP>:<PORT>/oo/hello.html

Load Balancer Security

In a hardened high availability environment, the load balancer should be configured for TLS. For information about how to configure TLS, see "Server and Client Certificate Authentication" in the *Operations Orchestration Securing and Hardening Guide*.

Communication between the Operations Orchestration interface and the load balancer can use HTTPS. We recommend to install the TLS certificate on the load balancer so that this is the termination point for the encryption. Beyond the load balancer, communication will continue in HTTP, at a faster rate.



Change from version 9.x: Unlike in previous versions, there is no need for external clustering software, nor is there a requirement for a shared file system.

Scalability

Operations Orchestration offers horizontal scaling for increasing execution throughput.

You can add more Central instances to the Operations Orchestration cluster. Operations Orchestration supports live scalability, which means that no downtime is required when adding a Central node. Simply install an additional Central instance and point it to the existing database schema.

For more information, see the *Operations Orchestration10 Benchmark* document, available on ITOM Marketplace at https://hpln.hpe.com/node/17617/attachment

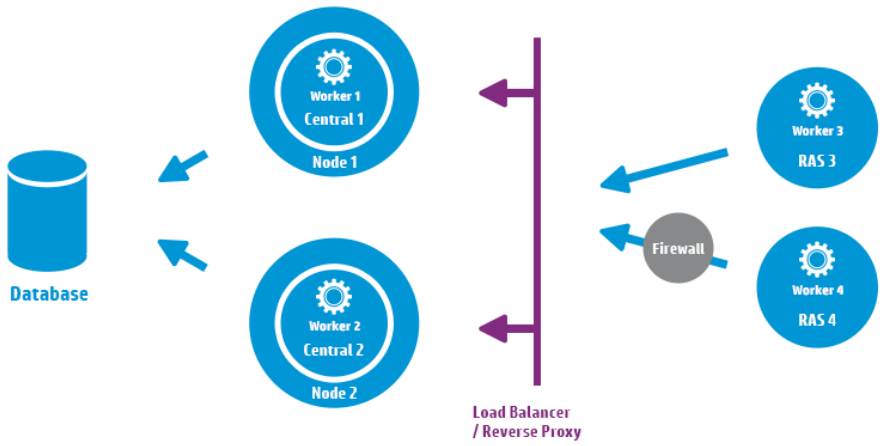
Adding an RAS

An RAS instance is an optional Operations Orchestration component. An RAS can be used if Operations Orchestration needs to run flows in a network segment that is not reachable from the Operations Orchestration Central nodes. In such case, you can install an RAS instance in the target network segment and it will pull the required flows from the Central and run them locally.

Another use case where a RAS can be used is when the executed flow requires specific binaries on the local machine. There is no need to install the binaries on each Operations Orchestration node. It is enough to install them on a host where a RAS is installed, and configure the flows (or specific steps) to run on this RAS. This can be achieved by leveraging the worker group functionality.

For more information on worker groups, see the *Operations Orchestration Concepts Guide*.

You can attach RAS instances to Central or a cluster of Central nodes. The image below shows how RAS3 and RAS4 communicate with the Central cluster. Note that RAS4 is located behind a firewall.



Configuring the RAS connectivity direction

In Operations Orchestration10.60 and later, you can configure RASes so that some initiate the connection to Central while others wait for Central to initiate the connection.

For example, if Central and a RAS are installed in different networks, with Central deployed on a more secured network, and your security rules do not allow connecting from the less secured network to the more secured one, you can have Central initiate the connection to the RAS.

During the installation of a RAS, you must choose between two options:

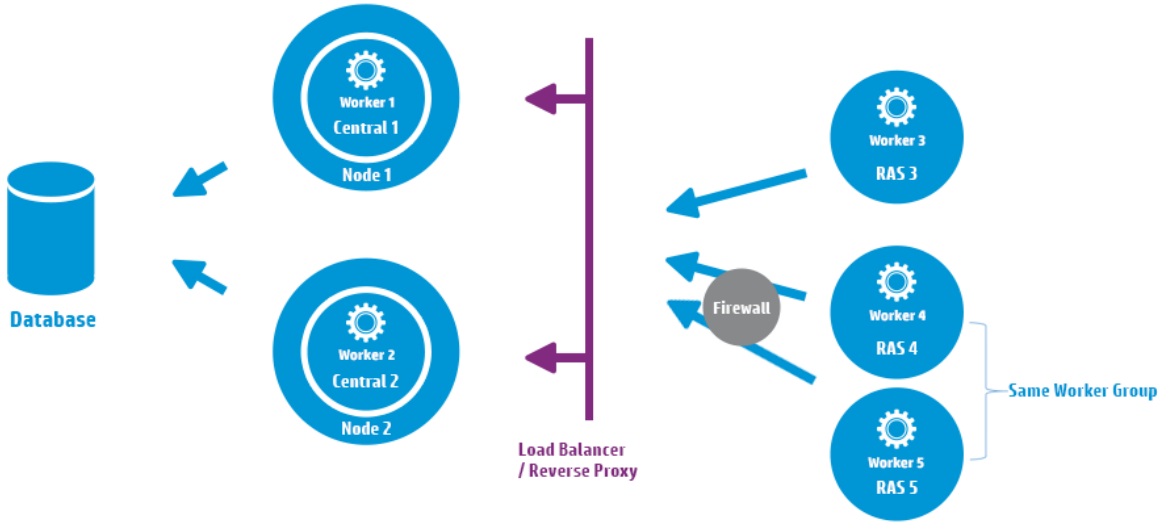
- **Standard RAS - RAS initiates communication to Central** - this is the simplest option and is recommended if your security rules permit it.
- **Reverse RAS - Central initiates communication to RAS** - choose this option if Central is installed in a different, more secured network, and your security rules do not allow connecting from the less secured network to the more secured one.

  You will need to configure the RAS to accept connection from Central, and configure Central to register the RAS (in the **System Configuration** > **Topology** > **Workers** tab).

  When the RAS starts up, it will be idle, waiting for Central to initiate connection.

RAS High Availability

When an RAS is deployed in a network segment to manage the machines in that segment, you do not have to make do with a single instance. To achieve high availability, you can deploy an additional RAS instance in the same segment. Make sure to associate it with the same worker group. This is illustrated in the image below:



Change from version 9.x: There is no need for an additional load balancer between the RAS cluster and Central (or central cluster). Because both RAS 4 and RAS 5 belong to the same worker group, they share the load of executing flows\steps that are designated for that worker group and provide high availability.

For information about how to install a load balancer, see the documentation provided by your load balancer vendor.

Configuring the Load Balancer and HPE operation orchestration Centrals for TLS offloading

If a load balancer is used to access the Central servers, it is recommended to configure the load balancer for TLS offloading.

1. Edit the Tomcat **server.xml** file, to include the following, for example:

```
<Engine name="Catalina" defaultHost= "localhost" >

. . .

<Valve
className="org.apache.catalina.valves.RemoteIpValve"protocolHeader="X-
Forwarded-Proto"   />

. . .

</Engine>
```

2. Configure the load balancer to add a new header to all the clients' requests.

   The header name is configurable and should match the Tomcat configuration specified above. In this example, the name is "X-Forwarded-Proto".

   In the F5 load balancer, the configuration would look like this:

```
when HTTP_REQUEST {

HTTP::header insert "X-Forwarded-Proto" "https";

}
```

Support Matrix

Operations Orchestration is a generic platform that can be installed in a variety of environments and used in various use cases.

Navigate through following topics to understand the hardware and software requirements to install the OO in different environments.

Software Requirements

Software Requirements for Central and RAS

The Central application requires a dedicated database schema.

Supported Operating Systems

OS	Version
Microsoft Windows Server	2016 64 bit 2008 64 bit, 2008 R2 64 bit 2012 64 bit, 2012 R2 64 bit
Oracle Enterprise Linux	6.6
Red Hat Enterprise Linux*	6.x 64 bit, 7.x 64 bit**
Ubuntu	14.04.x LTS

Note:

* **bzip2** is required when installing on RedHat systems. If it does not already exist on your Linux system, you can download it from http://www.bzip.org/downloads.html.

** Red Hat Enterprise Linux 5.x 64 bit is no longer supported.

Supported Databases

Database	Version
Oracle	12cR1 RAC, 12c R1 (regular, non-CDB), 11g R2, 11g R2 RAC
MySQL	5.5.x, 5.6.x*, 5.7x
PostgreSQL	9.1.x, 9.2.x, 9.3.x, 9.4x, 9.5x, 9.6
Microsoft SQL Server	2008 R2**, 2012**, 2014, 2016

* For MySQL 5.6.20 and 5.6.21, the requirements for the **innodb_log_file_size** have increased significantly. For MySQL 5.6.1 - 19, the recommendation is 256 M, but for MySQL 5.6.20 - 21, the recommendation is 2 GB.

** All service packs are supported.

Supported Browsers

Browser	Version
Microsoft Internet Explorer*	10.x, 11.x
Microsoft Edge	20
Mozilla FireFox**	32.x and later 31.x ESR (Extended Support Release) and later
Google Chrome**	40.x and later

* **Note**: Microsoft Internet Explorer 9.x is no longer supported.

** **Disclaimer**: Future versions of Firefox and Chrome are considered supported, subject to the browser's backward-compatibility.

Recommended screen resolution for the browser: 1280 x 1024 or 1920 x 1080

Other Requirements

Requirement	Version
.NET Framework	Microsoft .NET Framework 4.5 or later, full installation. This is also required for RAS installations.
Ports	Two ports must be available to configure for the Central Server (one for HTTP and one for HTTPS). The default values for these ports are 8080 and 8443, but you can specify different ports during installation. **Note:** It is also possible to change the ports after Operations Orchestration is installed. See "Changing or Closing the HTTP/HTTPS Ports" in the *Operations Orchestration Administration Guide.*

Software Requirements for Studio

Supported Operating Systems

OS	Version
Microsoft Windows	10, 8 64 bit, 8.1 64 bit, 7 64 bit*
Microsoft Windows Server	2016 64-bit, 2012 64 bit, R2 2012 64 bit, 2008 64 bit, R2 2008 64 bit

* **Note**: We no longer support Studio on Windows 7 32 bit.

Other Requirements

Requirement	Version
.NET Framework	Microsoft .NET Framework 4.5 or later, full installation. This is also required for debugging flows with .NET operations. If you don't have .NET 4.5, any flows or operations with .NET will be marked as invalid in Studio.
Service packs	Microsoft Visual C++ 2010 Redistributable Package (x86). This is required in order to use the Studio SVN integration feature. You need to download and install the version for the x86 platform, regardless of your Windows version (for example, if it is Windows x64). http://www.microsoft.com/en-us/download/confirmation.aspx?id=5555
Git client	In order to use the Studio Git integration feature, it is recommended to use version 2.9.2 of the Git client. For example: for x64: https://github.com/git-for-windows/git/releases/download/v2.9.2.windows.1/Git-2.9.2-64-bit.exe for x32: https://github.com/git-for-windows/git/releases/download/v2.9.2.windows.1/Git-2.9.2-32-bit.exe

Note: The minimum screen resolution for Studio is 1280 x 1024.

Software Requirements for the Database Server

Operating system support for database servers is according to the recommendations of the database vendor.

Hardware Requirements

The hardware requirements described here are the minimal supported configuration.

Many customers may require more powerful hardware, depending on their load and usage of the system. In some cases, scaling out (adding nodes) is preferable to scaling up (stronger hardware).

Hardware Requirements for Operations Orchestration Central and Database Servers

These requirements are for on-premise installations where the key components (central servers, RAS) are installed at the customer's site.

Component	Requirement per server (minimum)
CPU	**3 Gigahertz** (GHz) for single-processor systems or **2 GHz** for multi-processor systems Database server: • According to the database vendor's recommendations and requirements, but no less than **2 CPU cores** Central server: • Minimum: **1CPU core** • Recommended: **4CPU cores**
Memory (RAM)	Database server: • As specified by the vendor, but no less than **4 GB** Central server: • Minimum: **2 GB** • Recommended: **4 GB**
Hard-drive space	Database server: • Centralized database: ◦ **50 GB for Operations Orchestration data** - out of which a few GB are for the Operations Orchestration installation and content pack deployment, and the rest is used for Operations Orchestration's operational data. For extensive usage, it is recommended to allocate **100 GB** or more, depending on your data retention policy.

	• Dedicated database server:
	  ◦ **80 GB hard drive**
	  For extensive usage, it is recommended to allocate a **140 GB hard-drive** or bigger, depending on your data retention policy.

	Central server: • **2 GB**

For off-premise installations, where the key components are installed on a cloud-based virtualized machine, the hardware requirements are:

- Central/RAS: For Cloud systems, an extra small machine
- Database: According to the database vendor's recommendations and requirements, but no less than a small machine.

  For more information about database size requirements see the "Set Up Database Environment" in *Operations Orchestration Database Guide*.

Hardware Requirements for the Central Client

Web client machines for Central must meet the minimum hardware requirements for their web browser.

Hardware Requirements for RAS Installations

Component	Requirement (minimum)
CPU	**2 GHz** for single- or multi-processor systems Minimum: **1 CPU core** Recommended: **4 CPU cores**
Memory (RAM)	**1 GB**
Hard-drive space	**2 GB** (this includes room for the flows and operations that are included in the installation)

Hardware Requirements for Operations Orchestration Studio Installed on its Own Machine

Machines on which you install Studio must meet the minimum hardware requirements for their web browser or the following, whichever is higher.

Component	Requirement (minimum)
CPU	**2 GHz** for single- or multi-processor systems **1 CPU core**
Memory (RAM)	**2 GB** (this is the amount of memory that the Studio process requires)
Hard-drive space	**4 GB** (this includes room for the flows and operations in the installation)

Virtual Systems

Installation of the Operations Orchestration components on guest systems hosted by the following hypervisors is supported, as long as the guest systems meet the requirements described in this *System Requirements* document:

- VMware ESX Server, version 3.x or later
- Microsoft Hyper-V (for all supported Windows versions)

Cloud Deployments

Operations Orchestration can be installed on cloud computer units.

Performance and Sizing Information

This document aims to help the administrator to understand the different parameters that can impact system performance and to provide a set of tools for tuning the system in cases of less than optimal performance.

> **Note:** The appropriate tuning depends on how you use the system. If you change the parameters described in this document, you will need to monitor your system performance and re-tune if required.

Minimum Requirements

The minimal requirements for Operations Orchestration are described in the *Operations Orchestration System Requirements* document.

The requirements for database size are described in the *Operations Orchestration Database Guide*.

Parameters that May Affect your System Performance

This document aims to help the administrator in the process of tuning the system.

If you face a performance issue, you need to identify the cause or causes. This section lists the different parameters that might be impacting your system's performance.

It is recommended to read the list below, and to consider whether the various parameters apply to your use case. If so, click each relevant link to see more information about how to tune that parameter.

Performance may be affected by the following parameters:

- **Load** - A heavy load can exhaust the available resources (threads). This may be caused by running flows with a large number of parallel or multi-instance lanes, or by triggering a large number of flows simultaneously.

  In this case, the solution is to increase the number of threads. See "Increasing Number of Worker Threads" on the next page.

- **Memory consumption** - Your performance may be low because the JVM heap size is not appropriate and garbage collection is slowing down your system.

  It is recommended to analyze the time and frequency of garbage collection. You may need to adjust the initial and maximum size of the Central/RAS heap so that it is in accordance with your memory needs.

  See "Increasing the JVM Heap Size" on page 21.

- **Database size** - Operations Orchestration is database-intensive, and this may cause your database to become very large, and this will slow down performance.

  To keep your database is running efficiently, you need to purge it regularly to keep the size down. See "Purging the Database" on page 21.

  If you have other issues with your database, contact your database administrator or see the *Operations Orchestration Database Guide*

- **Run Log persistence level** - Your database may also be getting too large because of the run history that is persisted to the Run Log.

You can reduce the information that is saved by adjusting the persistence level in Central. See "Configuring the Amount of Data Written to the Database" on page 24.

- **Number of database connections** - Your system may be running slowly because either the Central server or the database server is limiting the number of concurrent connections.

  For more information about how to check whether the number of database connections needs tuning, and how to adjust this, see "Adjusting the Number of Database Connections" on page 23.

- **Number of Centrals** - If you have tried all the methods listed above and are still having performance issues, you may need to scale out, by installing additional Central servers or by adding more workers. Our recommendation is to add Central servers. See "Scaling Out " on page 25.

Increasing Number of Worker Threads

By default, each Operations Orchestration node has 20 worker threads. If your flows have a large number of parallel or multi-instance lanes, or if you trigger a large number of flows simultaneously, we recommend increasing this number. For example, you might increase this number to 200 threads per worker or Central.

> **Note:** The number of threads that can be configured is dependent on the amount of memory available to the Central or worker.

Increasing the Number of Worker Threads in Central or RAS

1. Open the **central-wrapper.conf** or **ras-wrapper.conf** file (located under **<installation_ folder>/central/conf** and **<installation folder>/ras/conf**, respectively) in a text editor.
2. To configure the number of execution threads, edit the property

   `-Dcloudslang.worker.numberOfExecutionThreads`

   The default value is 20.
3. To configure the size of the incoming buffer, edit the property

   `-Dcloudslang.worker.inBufferCapacity`

   The default value is 200.
4. Restart the configured node.

These are newly-supported properties. If this is the first time that you have configured them, you will need to add them manually as follows:

`wrapper.java.additional.<next available number>=`

```
-Dcloudslang.worker.numberOfExecutionThreads=<new value>
wrapper.java.additional.<next available number>=
-Dcloudslang.worker.inBufferCapacity=<new value>
```

Increasing the JVM Heap Size

You can adjust the initial and maximum size of the Central/RAS heap, so that it is in accordance with your memory needs and garbage collection is faster.

1. Open the **central-wrapper.conf** and **ras-wrapper.conf** files (located under **<installation_ folder>/<central or ras>/conf/)**.
2. Edit the following properties:

   ```
   wrapper.java.initmemory=<value in MB>
   wrapper.java.maxmemory=<value in MB>
   ```

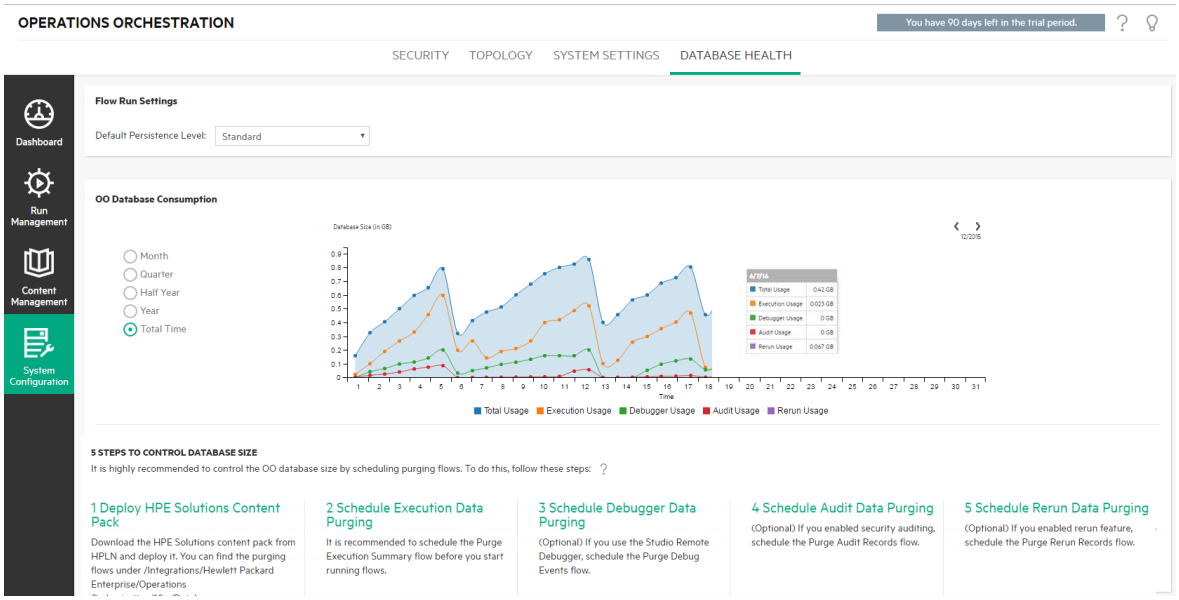
3. Restart the configured node.

Purging the Database

By default, Operations Orchestration 10.x saves all flow and step execution data in the database, in order to support debugging of flow runs. As a result, the database size will grow according to system throughput and flow complexity.

It is highly recommended to purge the database regularly, in order to control its size and enhance performance.

You can monitor the size of the database in Central, under the **Database Health** tab in the System Configuration workspace.



Purging Flows

The purging flows are available in the **HPE Solutions** content pack (available on ITOM Marketplace). It is recommended to deploy this content pack, configure the flows with your required settings, and schedule them in Central.

The following purging flows are located under **Library** > **Integrations** > **Hewlett-Packard Enterprise** > **Operations Orchestration** > **10.x** > **Database**:

- **Purge Execution Summary** - Purges run data.

  It is recommended to schedule this flow as soon as you start to run flows.

- **Purge Debug Events** - Purges Studio Remote Debugger event data.

  If you use the Studio Remote Debugger, schedule this flow.

- **Purge Audit Records** - Purges old auditing records if auditing is enabled.

  If you have enabled security auditing, schedule this flow.

- **Purge Rerun Info** - Purges rerun data.

  If you have defined rerun points in your flows, schedule this flow.

For more information about these purging flows, see the flow descriptions in Central.

Purging APIs

As an alternative to using the purging flows, you can perform purging functions via API.

The following APIs are available:

- **DELETE /audit/records**: Purges old auditing records if auditing is enabled.
- **DELETE /debugger-events**: Purges Studio Remote Debugger event data.
- **DELETE /executions**: Purges run data such as bound inputs, outputs and step log events. This run data needs to be purged regularly, because running large numbers of runs can cause the database to reach the maximum table size.

  > **Note:** This only affects the data of completed runs.

- **DELETE/executions/rerun**: Purges the rerun data from the database.
- **DELETE /steps-log**: Purges step data according to time and number of executions to purge.

By using the purge APIs, you can purge the data manually as required, or by scheduling recurrent flows that incorporate these APIs.

Adjusting the Number of Database Connections

Your system may be performing badly because the minimum and maximum database connection pool size is not set correctly.

Analyzing Whether You Need to Adjust the Database Connections

To identify if the number of database connections is an issue in your environment:

1. Open the **database.properties** file (located under **<installation_folder>/central/conf/**), and register the value of the `db.pool.minPoolSize` and `db.pool.mxPoolSize` properties.

   The Central server aims to keep the number of database connections at the defined minimum value. If necessary the Central server will add connections but will not exceed the maximal value.

2. Review your database server configuration and check the current limitation on the number of database connections.

   Note that in some cases, this limitation is global (the sum of all connections to all database schemas) and in other cases, resource-usage profiles may apply. Consult your DBA, in that case.

3. Connect to the database server and track the number of connections from this Central server to the database throughout busy hours. It is important to count only the connections that originated from this specific Central server.

If you are using an Operations Orchestration cluster, you must configure the database server to allow connections from a number of Central servers, as well as connections from other clients and consumers.

Changing the Number of Database Connections

In order to change the maximum number of database connections on the Central server's end:

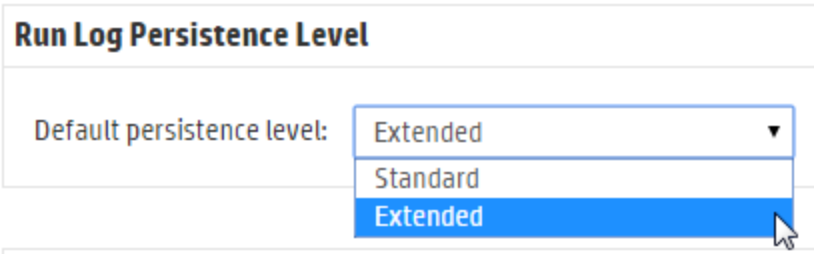
1. Open the **database.properties** file (located under **<installation_folder>/central/conf/**).
2. Edit the `db.pool.maxPoolSize` property.
3. Restart the configured node.
4. Repeat for every Central node.

Configuring the Amount of Data Written to the Database

In Central, a very detailed run history is persisted. This makes it easy to troubleshoot, as all the information is available in the Run Log. However, if your database size has increased to the limit, you may need to reduce the information that is saved to the Run Log.

Two persistence levels are available, and each one saves a different set of data:

- **Standard** - large input/output values are truncated at approximately 4,000 bytes when logged
- **Extended** - large input/output values are not truncated when logged



Under the **Database Health** tab in the System Configuration workspace, select the default log level. This will be applied, by default, to all flows that are run.

You can override this default for individual flows in the flow library, or when triggering or scheduling a flow run.

You can also set the log level in API runs (REST/SOAP).

Scaling Out

Scalability is the ability of the Operations Orchestration system to be enlarged to accommodate a growing amount of work, so that it increases its total throughput under an increased load.

Adding More Central Servers

To way to scale out is to install additional Central servers in an Operations Orchestration cluster.

Clustering provides high availability and scalability to enhance throughput. To create a cluster, you run the Installation wizard to create the first Central. Then, you run it again on the other machine to create the next node and, during this second installation, make it point to the same database schema.

For more information, see "Installing an Operations Orchestration Central Cluster" in the *Operations Orchestration* *"Install" on page 4*.

Adding More Workers

Another method of scaling out is to add more workers to the existing Operations Orchestration Central server.

Workers are responsible for executing flows. An external worker connects to Central to obtain tasks (flow execution messages) to process.

To create a new worker, install a new RAS. For more information, see "Installing a RAS" in the *Operations Orchestration* *"Install" on page 4*.

Pre-Installation Tasks

This section provides information on how to setup the required environment before installing Operations Orchestration.

Before installing Operations Orchestration, you must download and install Microsoft Visual C++ 2010 Redistributable Package (x86). You need to install the version for the x86 platform, regardless of your Windows version.

This package can be downloaded from: http://www.microsoft.com/en-us/download/confirmation.aspx?id=5555.

- It is recommended to install Operations Orchestration on a secured environment.
- If you are installing Central with MySQL, you will need to provide the MySQL JDBC driver. Use MySQL Connector release 5.1.35.

This driver can be downloaded from:

http://mvnrepository.com/artifact/mysql/mysql-connector-java

- If you are installing Central with Oracle, you will need to install the Oracle JDBC driver. Download the JDBC driver from http://www.oracle.com/technetwork/database/features/jdbc/default-2280470.html.

  It is recommended to use Oracle JDBC driver version 7-12.1.0.2.

  If you are performing a silent installation, set the value of the `db.driver.location` parameter to the path of JDBC driver in the **silent.properties** file.

- Before installing Operations Orchestration, make sure to back up your system. Consult with your system administrator.
- If you uninstalled a previous version of Operations Orchestration and are installing 10.x in the same installation folder, make sure to back up the all the files that were under the installation folder and delete that folder before installing the new version.
- The Central server requires two ports, so make sure that two ports are available.

  > **Note:** The default ports are 8080 and 8443, but you can use any two available ports.

SQL Scripts to Create the Database Objects

If, for security reasons, the Operations Orchestration database user lacks the ability to create objects such as tables, indexes, sequences, and so on, you can use SQL scripts from the ZIP file to manually create the database objects using an elevated privileges database connection.

Before using these scripts, you need to have the database or schema already created. The scripts to create the database or schema can be found in the "Manually Creating an Operations Orchestration Database" sections of the *Operations OrchestrationDatabase Guide* document.

The SQL scripts are located at **\docs\sql** on the ZIP file. They include:

- mssql.sql
- mysql.sql
- oracle.sql
- postgres.sql

Database-specific Adaptations

This section describes several key database-specific adaptations and requirements. For detailed instructions, see the *Operations Orchestration Database Guide*.

- **MySQL**: If you are deploying Operations Orchestration using a MySQL database, you need to configure the MySQL server configuration file **my.ini** (Windows) or **my.cnf** (Linux) with the following options:

```
transaction-isolation = READ-COMMITTED
default-storage-engine = INNODB
character-set-server = utf8
max_allowed_packet = 250M
innodb_log_file_size = 256M
max_connections = 1000
```

- **Postgres**: If you are deploying Operations Orchestration using a Postgres database, you need to configure the Postgres server configuration file **postgresql.conf** with the following options:

```
default_transaction_isolation = 'read committed'
autovacuum = on
track_counts = on
max_connections = 1000
```

- **Oracle**:

  If you are deploying Operations Orchestration using an Oracle database, you need to configure the Oracle server PROCESSES and OPEN_CURSORS to guarantee up to 1000 concurrent connections for Operations Orchestration and up to 900 open cursors per session.

- **SQL Server**

  If you are deploying Operations Orchestration using an SQL Server database, you need to set the following options for the database:

```
ALLOW_SNAPSHOT_ISOLATION        ON
READ_COMMITTED_SNAPSHOT         ON
AUTO_CREATE_STATISTICS          ON
AUTO_SHRINK                     OFF
```

Installation Tasks

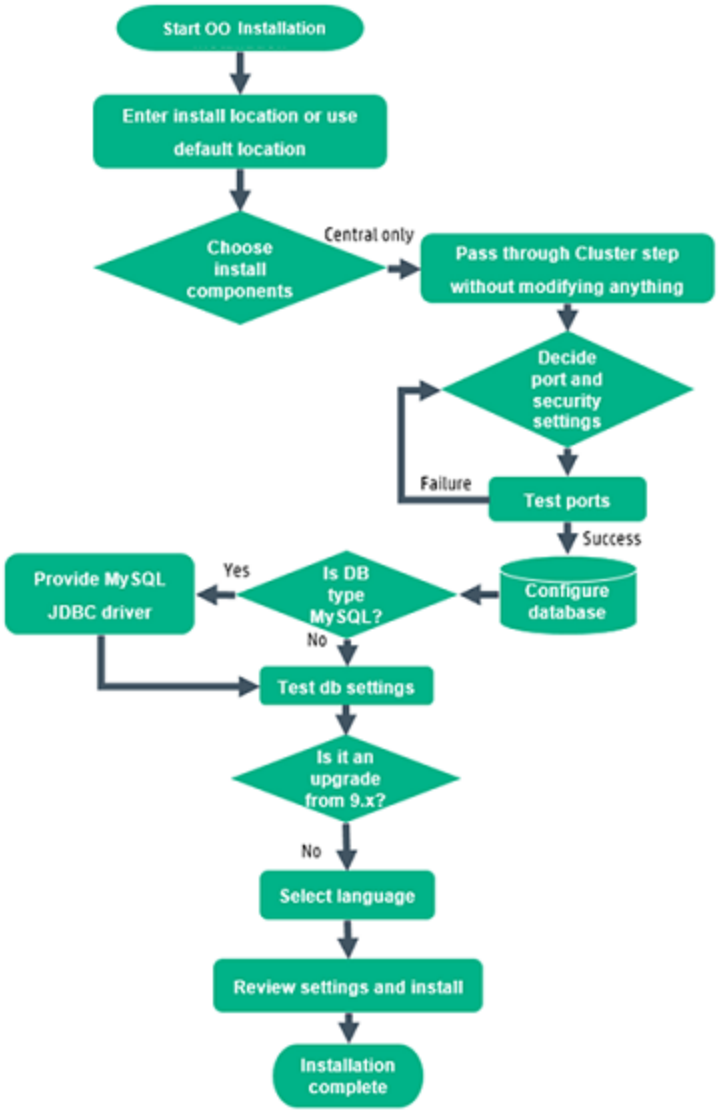
This section includes descriptions of how to install Operations Orchestration Studio and RAS .

First, see the **"Pre-Installation Tasks" on page 25**. Then, go to the relevant installation section:

Installing Operations Orchestration Central with Installation Wizard

> This section is applicable only if you install Operations Orchestration 10.80 in Standalone mode. This is not applicable if you install Operations Orchestration as a container as part of suite installation.

This section describes how to perform a clean installation of a single Central on Windows or Linux. In some cases, the screenshots display the Windows information. Click each node on the map to jump to the relevant topic.

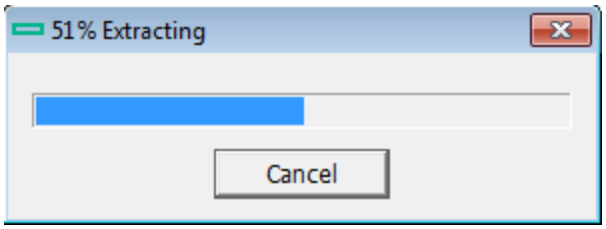


Start the Operations Orchestration Installation

1. Download the ZIP file from the HPE SSO Portal and extract it into a local drive on your computer.
2. To start the installer:
   - On Windows: Double-click the **installer-win64.exe** installation file.
   - On Linux: Run this command from a Linux desktop/an X-Window terminal:

     ```
     bash installer-linux64.bin
     ```

     To start the installer, double-click the **installer-linux64.bin** file.
3. After you start the installer, the installation package is extracted, and the **Operations Orchestration Installation and Configuration Wizard** automatically opens. Click **Next**.



4. In the **License** page, select **I Agree**, and then click **Next**.

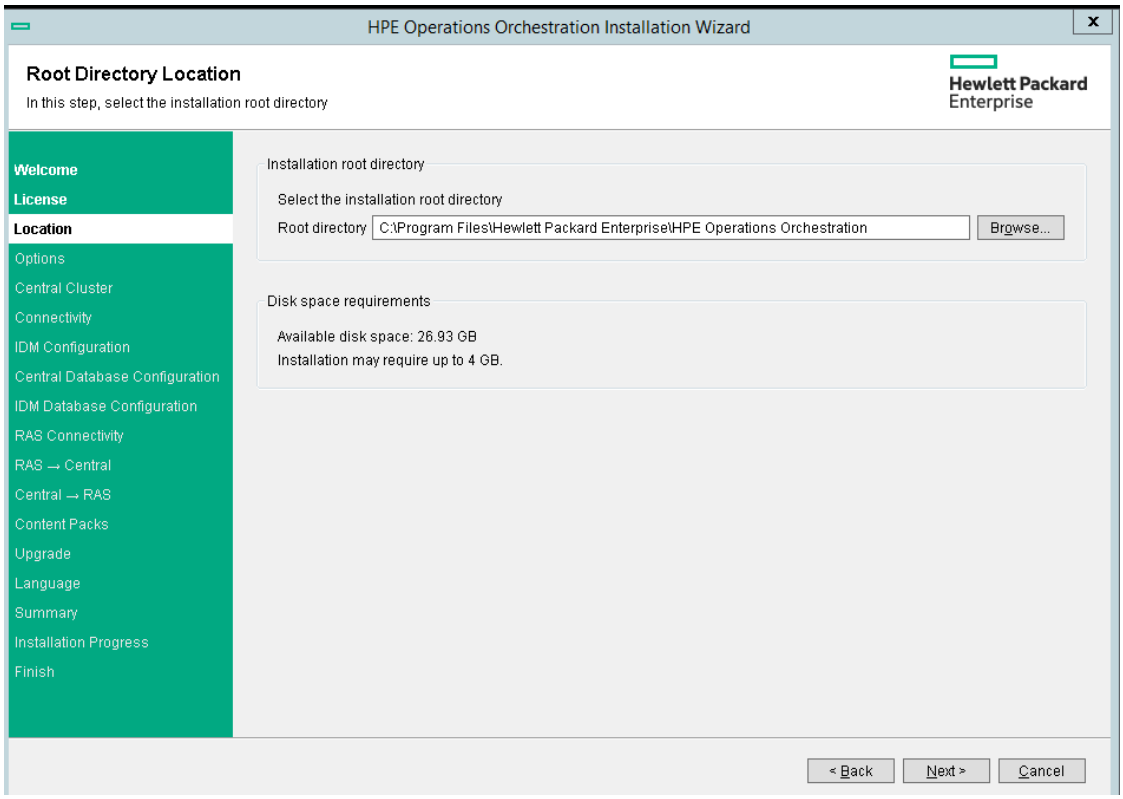
Back to the flowchart

Enter the Installation Location or Use the Default Location

1. In the **Location** page, select the location for the installation root directory.

   If the directory does not exist, the directory is created automatically. You are prompted to confirm the creation of the new location.

   > **Note:** Valid characters for the installation path are English letters, digits, spaces, hyphens (-) and underscores (_).
   >
   > The default path is `C:\Program Files\Hewlett-Packard Enterprise\HPE Operations Orchestration` for Windows and is `/opt/hpe/oo` for Linux.



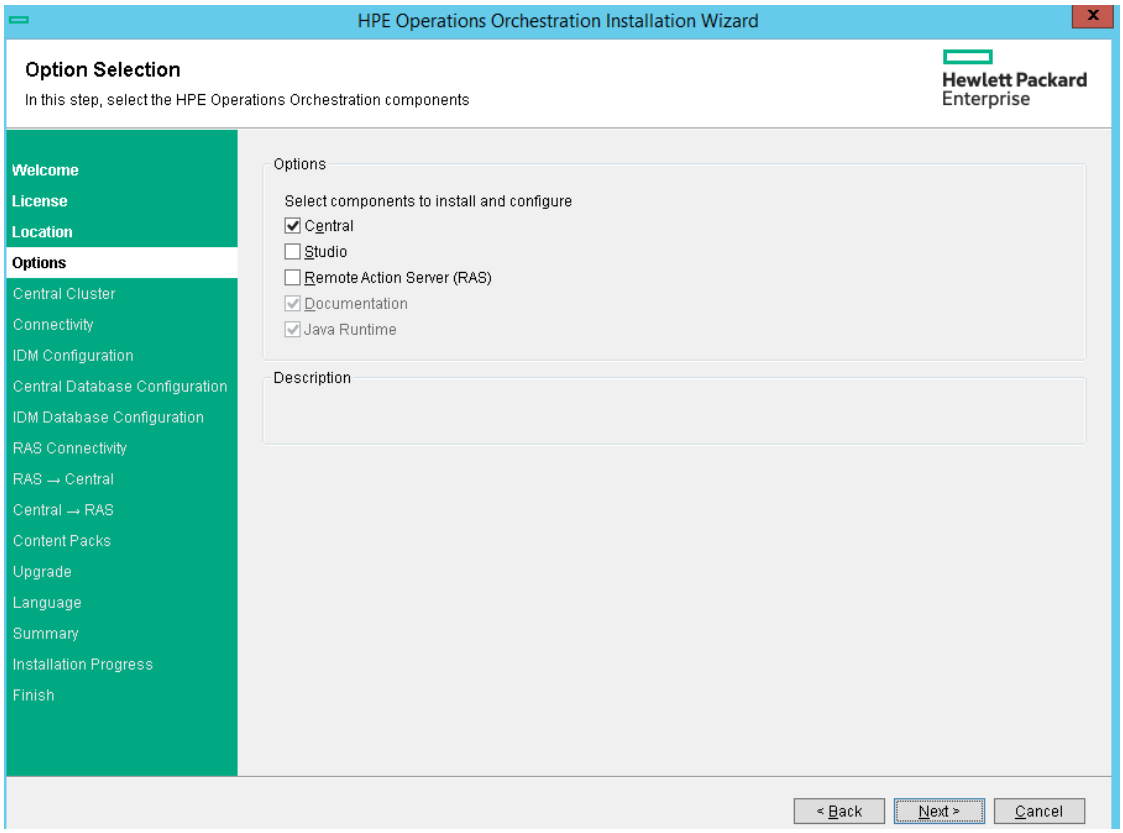
2. Click **Next**.

Back to the flowchart

Choose the Installation Components

1. In the **Options** page, select **Central**.

> **Note:** You can install Central without setting up a RAS server. If you install a RAS Server, it is recommended that you install this on a separate server to Central. See "Installing Operations Orchestration RAS Using the Installation Wizard" on page 50.



2. Click **Next**.

Back to the flowchart

Pass Through the Cluster Step Without Modifying Anything

In the **Central Cluster** page, click **Next**.

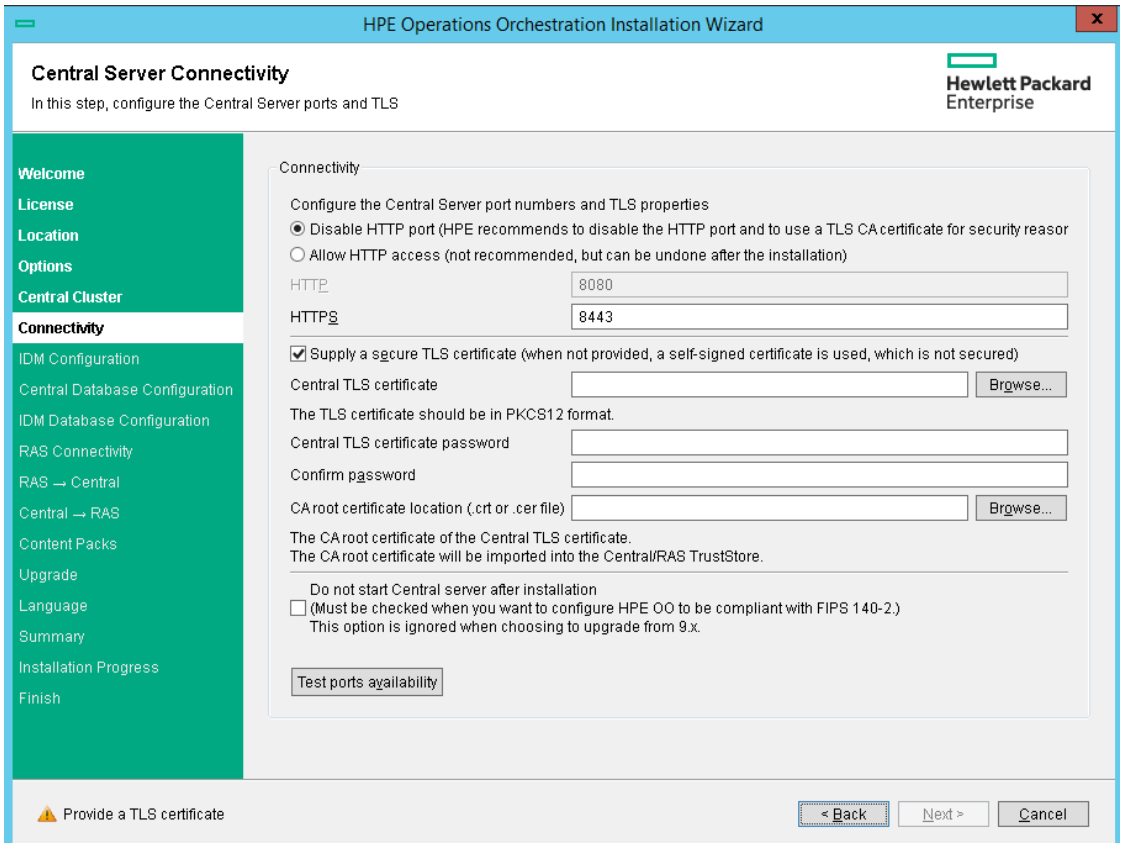
For information about how to install a node in a cluster, see "Installing an Operations Orchestration Central Cluster" on page 90.

Back to the flowchart

Decide Port and Security Settings

In the **Connectivity** page, configure the Central Server ports and TLS:

1. Configure available ports for the Central Server. Default values (8080 and 8443) appear for each port, but you can change these. Choose one of the following options:



- (Recommended) Select **Disable HTTP Port** and configure a port in the **HTTPS** field.

  This option is recommended for security reasons, so that the communication channel is encrypted.

- (Not recommended) Select **Allow HTTP access** and configure two ports in the **HTTP** and **HTTPS** fields.

> **Note:** Configuring at least one port is mandatory. If a port is not defined, or if the ports are occupied by other applications, you will not be able to complete the installation.

2. (Recommended) Select **Provide a secure TLS certificate**, and then click **Browse** to select the certificate.

   This step is recommended, for security reasons. If you do not select a Central TLS certificate, Operations Orchestration uses a self-signed certificate.

> **Note:** Do not use a network path for the location of the Central TLS certificate.

3. If you selected a Central TLS certificate, enter its password, and enter it again for confirmation.

4. Click **Browse** to specify the location of the CA root certificate, which will be imported into the TrustStore for Central/RAS.

   > **Note:** Do not use a network path for the location of the CA root certificate.

5. Select **Do not start Central server after installation** if either of the following is true:
   - If you are configuring Operations Orchestration to be compliant with FIPS 140-2.
   - If you are installing a new Central in cluster mode and the installer version is older than the current Central.

     > **Note:** If you are installing Central and RAS together, or upgrading from 9.x, this option is not available. This is because the RAS server needs to connect to the Central server. If Central is not started, the installation of the RAS will fail.

Back to the flowchart

Test the Ports

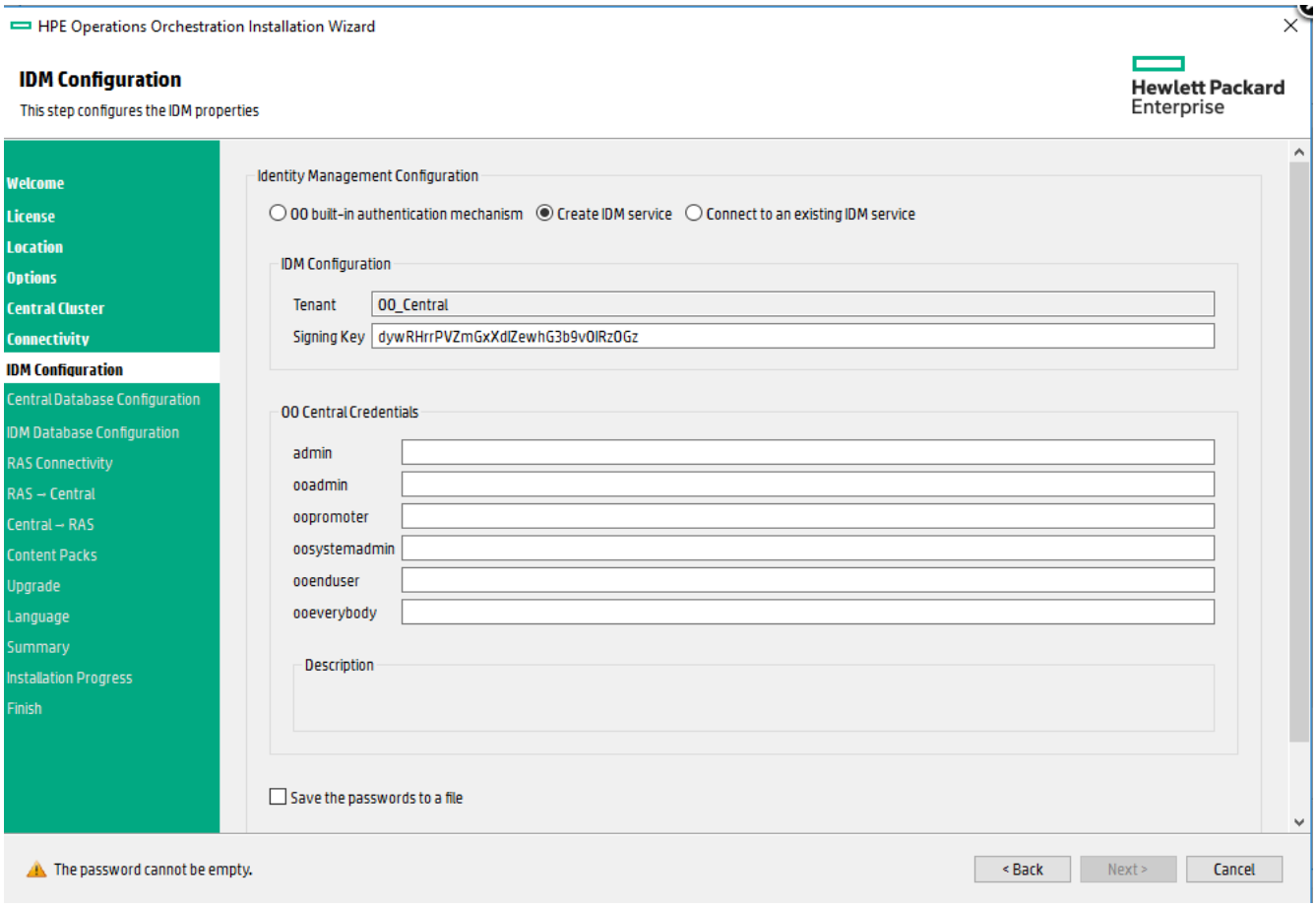
Click **Test ports availability**. If the ports are available, a **Success** check mark appears.

- If you encounter an error, adjust the ports accordingly and try again.
- If the **Success** check mark appears, click **Next**.

Back to the flowchart

Configure IDM

In the **Identity Management Configuration** page, you can install a centralized Identity Management Service (IDM) or you can connect to an existing IDM service. You can also choose to use the OO built-in authentication.



If you choose to create an IDM service, perform the following steps:

1. In the **Tenant** field, enter the value of the tenant to be configured in the IDM service. The default value fis "OO_Central".
2. In the **Signing Key** field, enter the value of the IDM configuration signing key. The signing key must be at least 32 characters and must contain lower case, upper case, and numeric letters.
3. In the **OO Central Credentials** area, **admin** field, enter the administrator user name of the IDM integration account.
4. In the **ooadmin** field, , enter the password for the user who has the SUPER_IDM_ADMIN role. This user is an elevated API user and is used only for API calls between Operations Orchestration and IDM. This user is not to be used to log in to Operations Orchestration as the role assigned to the user is "OO is END_USER".
5. In the **oopromoter** field, enter the password for the user with the PROMOTER role. This user can access the Content Management and Run Management workspaces.

6. In the **oosysadmin** field, enter the password for the user with the SYSTEM_ADMIN role. This user can access the System Configuration and the Run Management workspaces.
7. In the **ooenduser** field, enter the password for the user with the END_USER role. This user can access only the Run Management workspace.
8. In the **ooeverybody** field, enter the password for the user with the EVERYBODY role. This user can access only the Run Management workspace.
9. Select the **Save the passwords to a file** check box if you want save the information in this screen to a file. If you select the check box, browse and select a file in which information from this page will be saved. The default IDM transport user and IDM transport password are also saved in this file (`idm.configuration.username` and `idm.configuration.password`).

If you choose to connect to an existing IDM service, perform the following steps:

1. In the **IDM URL** field, enter the he URL of the IDM service.

   For example, <idm_protocol>://<idm_hostname>:<idm_port>/<idm_service_path>
2. In the **IDM Transport Username** field, enter the user name of the IDM REST integration.
3. In the **IDM Transport Password** field, enter the IDM REST integration password.
4. In the **Signing Key** field, enter the signing key for the IDM configuration. The signing key must be of at least 32 characters and must contain lowercase, uppercase, and numeric letters.
5. In the **Tenant Credentials** area, **Tenant** field, enter the tenant value of Central to be configured in the IDM service. The default value "OO_Central".
6. In the **IDM Administrator Username** field, enter the user name of the user with full access to the IDM database.
7. In the **IDM Administrator Password** field, enter the password of the IDM administrator user.

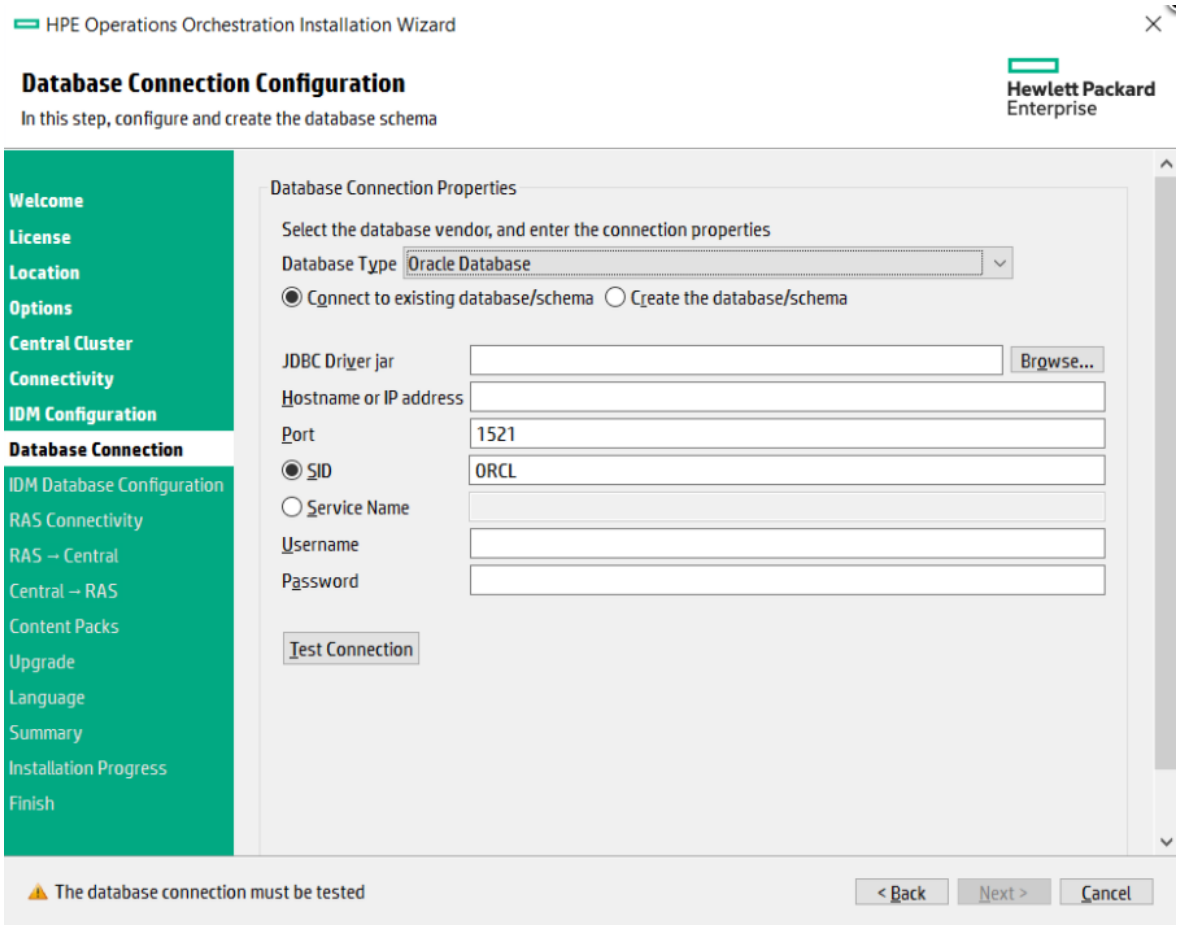
You must create a new database for the IDM component and provide the authentication details of the user with access to that database.

Back to the flowchart

Configure the Database

In the **Central Database Connection** page, you configure and create the database schema.

> **Note:** If you have user input in two languages apart from English (for example, German and Chinese) then MS SQL should not be used. You should use an alternative database such as Oracle, MySQL, or Postgres with the recommended Unicode configuration for Operations Orchestration.



1. From the **Database Type** list, select the database vendor, and then enter the connection properties.

   > **Note:** When the **Connect to existing database/schema** option is selected, do not use administrative user accounts in the **Username** and **Password** fields, because this will install Operations Orchestration under the administrative account.
   >
   > When the **Create the database/schema** option is used, provide a user with the relevant privileges in the **Admin username** and **Admin password** fields.

   You can select from the following database types:

   - **Oracle**: Do not use **SYS**, **SYSTEM**, or other administrative accounts credentials in the **Username** and **Password** fields.

     > **Note:** If you are using Oracle 11g R2 or 11g R2 RAC, it is recommended to apply patch 20299013 before installing Operations Orchestration.

   - **Microsoft SQL Server**: Do not use **sa** or other administrative account credentials in the

Username and **Password** fields.

- **Oracle MySQL**: Do not use the **root** credential in the **Username** and **Password** fields.

  If you are installing Operations Orchestration with Oracle RAC (Real Application Cluster), you must choose **Other database** and provide the URL.

- **PostgreSQL**: Do not use the **postgres** credential in the **Username** and **Password** fields.

  > **Note:** PostgreSQL database names are case-sensitive.

- **Internal database**: This uses an H2 local database. This should not be used for production.
- **Other database**: (use to enable advanced features in supported databases). If you select **Other database**, you can only use a database type that is supported for use with Operations Orchestration.

  > **Note:** The **Other database** option also supports any valid JDBC URL.

2. After selecting the database type, select one of the following:
   - **Connect to existing database/schema**: Connect to an existing schema, user, or database. The installer verifies that the schema/database and user exist.
   - **Create the database/schema**: Enables you to create a new database or schema. Information in the **Database**, **Username** and **Password** fields will be used in order to create the new schema, user, or database for Operations Orchestration.

     Confirm the password by typing it again in the **Confirm Password** field.

     Important! Make sure to use a strong password, in accordance with your organization's security policy. If the password is not strong enough, an error message will appear.

     Provide existing database user credentials in the **Admin username** and **Admin password** fields. This elevated-privileges user must be able to connect to the database and create the new schema, user, or database for Operations Orchestration.

     DBA (Admin) credentials will only be used for creating the Operations Orchestration database and user/role. It is completely safe to provide these credentials, as they not saved and not used after the Operations Orchestration installation.
3. Select the path to the Oracle JDBC driver that you installed as part of the "Pre-Installation Tasks" on page 25.
4. Enter the hostname or IP address and other connection details.

   Make sure to use the FQDN (Fully Qualified Domain Name).

If you want to use IPv6, put the IPv6 address in brackets, for example, [3fff::20]. Otherwise, errors will occur.

5. (For Oracle) Select either **SID** or **Service Name**, and enter the SID or service name of the database.

   It is recommended to use Oracle database's service name rather than using the SID.

   > **Note:** If you are upgrading from a 9.x version that is installed on Oracle, you must enter the SID of this database in the **SID** field, and not the database name.

Back to the flowchart

Is the Database Oracle or MySQL?

Yes: Go to Provide the JDBC Driver for Oracle or MySQL

No: Go to Test Database Settings

Provide the JDBC Driver for Oracle or MySQL

Complete this step if the database is Oracle or MySQL:

In the **Database Connection** page, click **Browse** and select the location of the JDBC driver.

Back to the flowchart

Test the Database Settings

Click **Test Connection**. If you are unable to connect to the database, you will not be able to proceed to the next steps in the wizard.

If your password is not strong enough, a warning is displayed. You will still be able to proceed with the installation, but it is strongly recommended to replace it with a stronger password.

The installer checks for non-empty schemas/databases, and shows a warning message if the schema or database is not empty. If the installation fails during schema validation, the installation process is stopped.

> **Note:** This test only verifies the connection between Operations Orchestration and the selected database, and does not verify the conditions required by the database, like the user's read/write permissions on the provided schema.

> **Note:** For all the database vendors, if you select to create a new database, the created database uses **case-sensitive** collation as follows:

- MySQL: **utf8_bin collation** is used for the new database.
- Postgres: Case-sensitive by design. No need for specific settings. **UTF-8** encoding is supported
- Oracle: Case-sensitive by default. No need for specific settings. **UTF-8** encoding is supported.
- MS SQL: Use only the following database collations per your required language:
  - English: SQL_Latin1_General_CP1_CS_AS
  - Japanese: Japanese_Unicode_CS_AS
  - Simplified Chinese: Chinese_Simplified_Stroke_Order_100_CS_AS
  - German: SQL_Latin1_General_CP1_CS_AS
  - French: French_100_CS_AS
  - Spanish: SQL_Latin1_General_CP1_CS_AS

However, if you already have a database installed, Operations Orchestration creates the tables using the database specific collation. It is important to note that using other collations can cause characters to appear in gibberish in the user interface for localized installations. In addition, other collations are not officially supported in Microsoft SQL Server for localized installations.

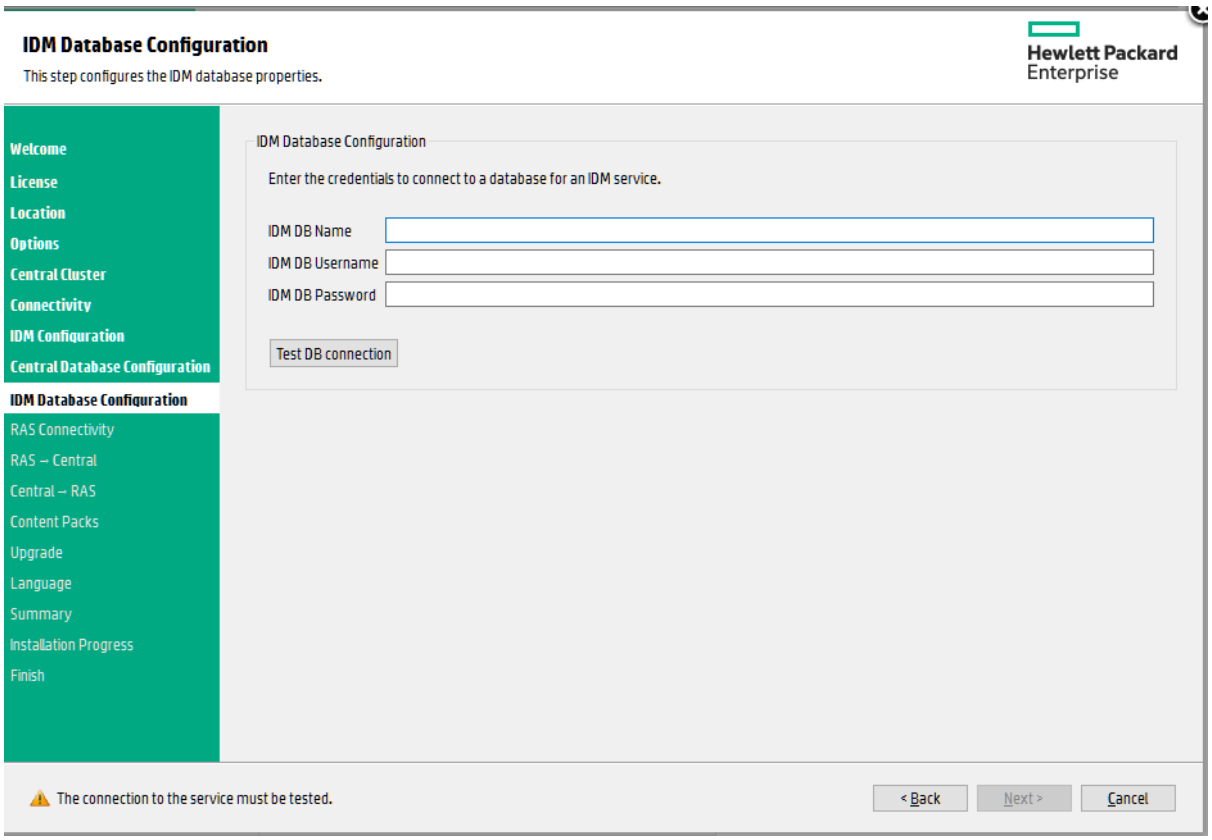
If the installer is used in order to create a new SQL Server database, selecting your language in the language selection page sets the correct collation for the new database.

Using one of the above collations enables using the **varchar** datatype for textual columns instead of the **nvarchar** data type. Using the **varchar** data type is more efficient and reduces overall database size.

Selecting a specific language also means that an Operations Orchestration system that uses SQL Server is limited to the set of languages supported by that specific collation. For example, if the **SQL_Latin1_General_CP1_CS_AS** collation is used, English, German, and Spanish characters may be used, but Japanese characters may not. If **Japanese_Unicode_CS_AS** is used, French accent characters will not be presented properly. For the complete specification of each collation, see the Microsoft SQL Server documentation.

Back to the flowchart

Configure the IDM Database



If you had selected MY-SQL as the database type previously, you must set the variable `lower_case_table_names` to `1`.

If you plan to set the `lower_case_table_names` system variable to `1` on Unix systems, you must first convert your old database and table names to lowercase before stopping `mysqld` and restarting it with the new variable setting. You must make sure that all applications using the database support this setting.

Note: The IDM database that you are configuring must be empty. If the IDM database is not empty, a warning message is displayed when testing the connection.

1. (For Oracle) Select either **SID** or **Service Name**, and enter the SID or service name of the database. The default SID value is "ORCL".
2. In the **IDM DB Name** field, enter the database name created for IDM service.
3. In the **IDM DB Username** field, enter the user name of the user with full access to the IDM

database.

4. In the **IDM DB Password** field, enter the password for the specified user.

Is it an Upgrade from 9.x?

In the **Upgrade** page, click **Next** without modifying anything.

This procedure describes how to perform a clean installation of Operations Orchestration10.x. For information about upgrading from 9.x, see the document *Upgrading to Operations Orchestration 10.x from 9.x*.

Back to the flowchart

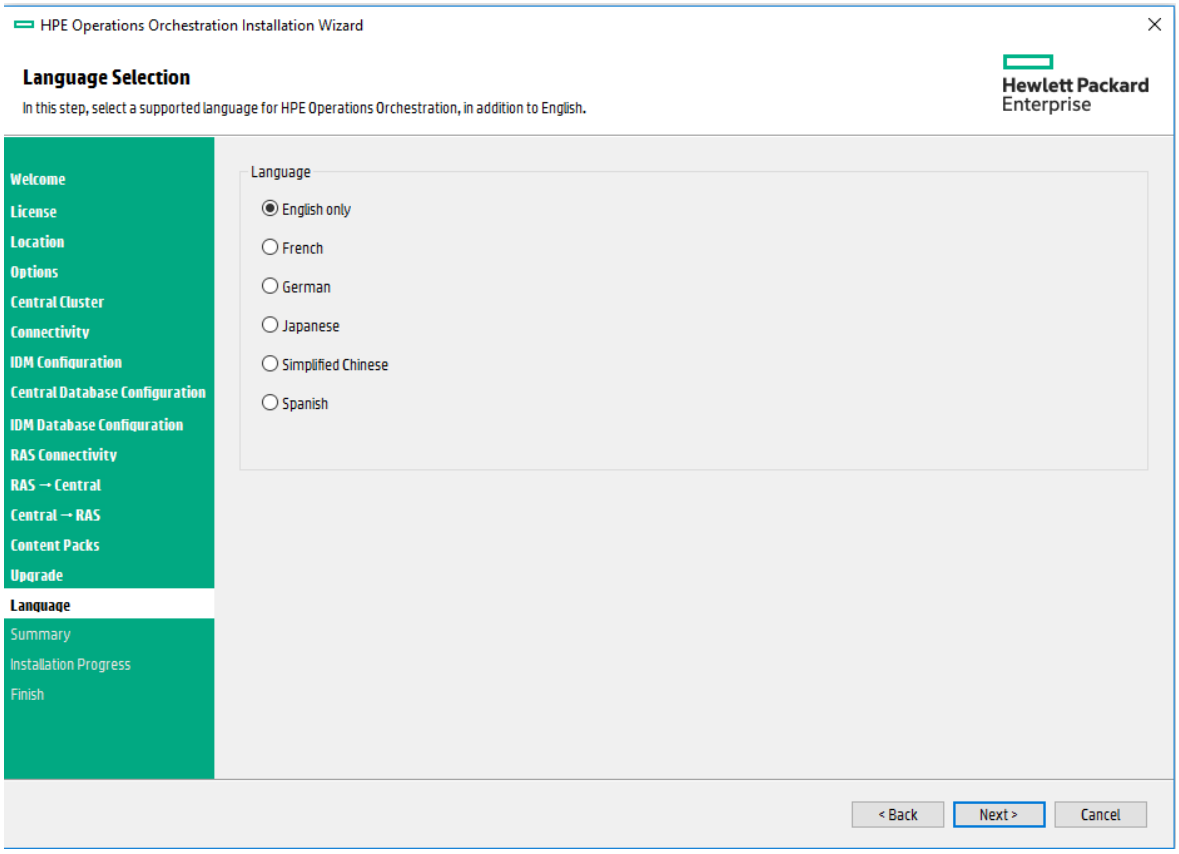
Select the Language

In the **Language** page, select a supported language for Operations Orchestration, in addition to English, and then click **Next**.

This language support will be used for:

- The MS SQL collation language, if relevant
- The **central-wrapper.conf** language for content. This language support may be required if, for example, you need to ping a server that is configured in Japanese.

> **Note:** You can change the language support choice after installation, by editing the **central-wrapper.conf** file, located in the installation directory under **central/conf**.



Back to the flowchart

Review Settings and Install

1. The **Summary** page displays the installation and configuration settings that you selected and entered in the wizard. Check that the settings are correct. If you want to correct one of the items, click **Back**.
2. Click **Install**. The installation begins, and the wizard displays a check mark next to each successfully installed item on the **Progress** page. When the installation is complete, click **Next**.

   > **Note:** If there is a problem with one of the installation or configured items, the installation attempts to continue with the rest of the items regardless of that error. Check the **installer.log** file (the default located is **C:\HPE\oo** for Windows or in **/HPE/oo** for Linux), to check for errors.

3. (Optional) In the **Finish** page, select **Open Welcome Page** to display the Operations Orchestration Welcome page in your default web browser, in the language that was selected on the **Language** page.
4. Click **Finish** to close the Installation and Configuration wizard.

Installation is Complete

Central is installed and menu shortcuts are created on your system.

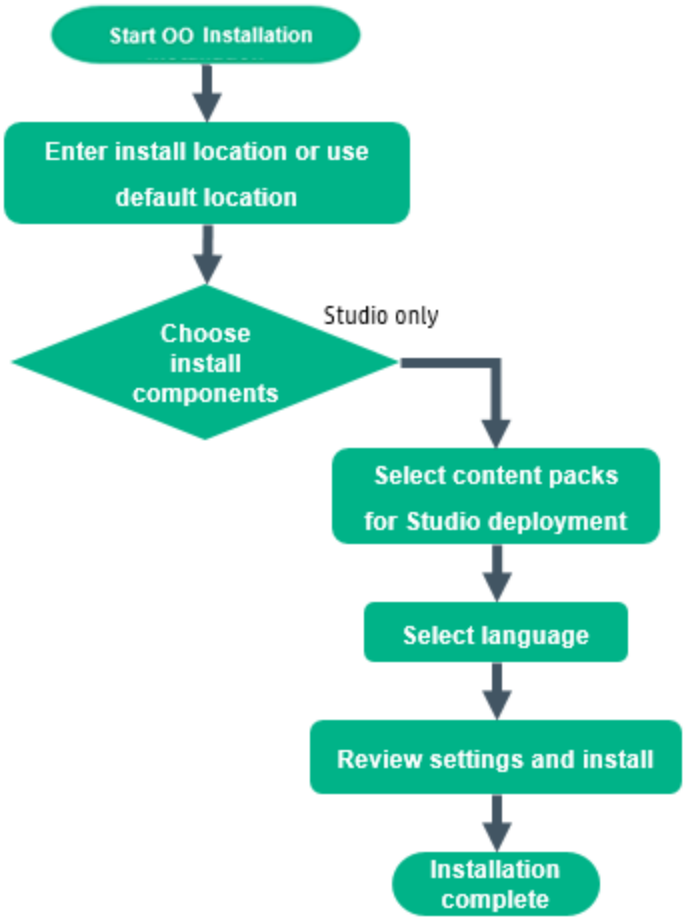
The installation is of the Trial version of Operations Orchestration. As a result, you will need to install the Enterprise Edition license within 90 days. You will need to generate the license with the IP of the Central server.

Installing Operations Orchestration Studio Using the Installation Wizard

> This section is applicable to both Standalone and Containerized installation.

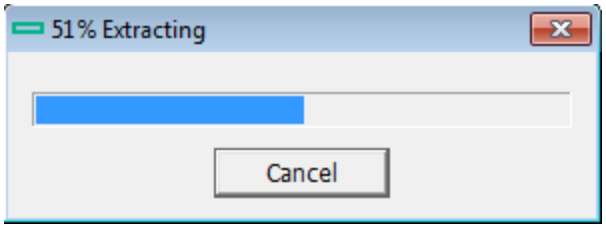
This section describes how to perform a clean installation of Operations Orchestration Studio.

> **Note:** Studio only works on Windows, so it cannot be installed on Linux.



Start the Operations Orchestration Installation

1. Download the ZIP file from the HPE SSO Portal and extract it into a local drive on your computer.
2. To start the installer, double-click the **installer-win64.exe** installation file.
3. After you start the installer, the installation package is extracted, and the Operations Orchestration **Installation and Configuration Wizard** automatically opens. Click **Next**.



4. In the **License** page, select **I Agree**, and then click **Next**.

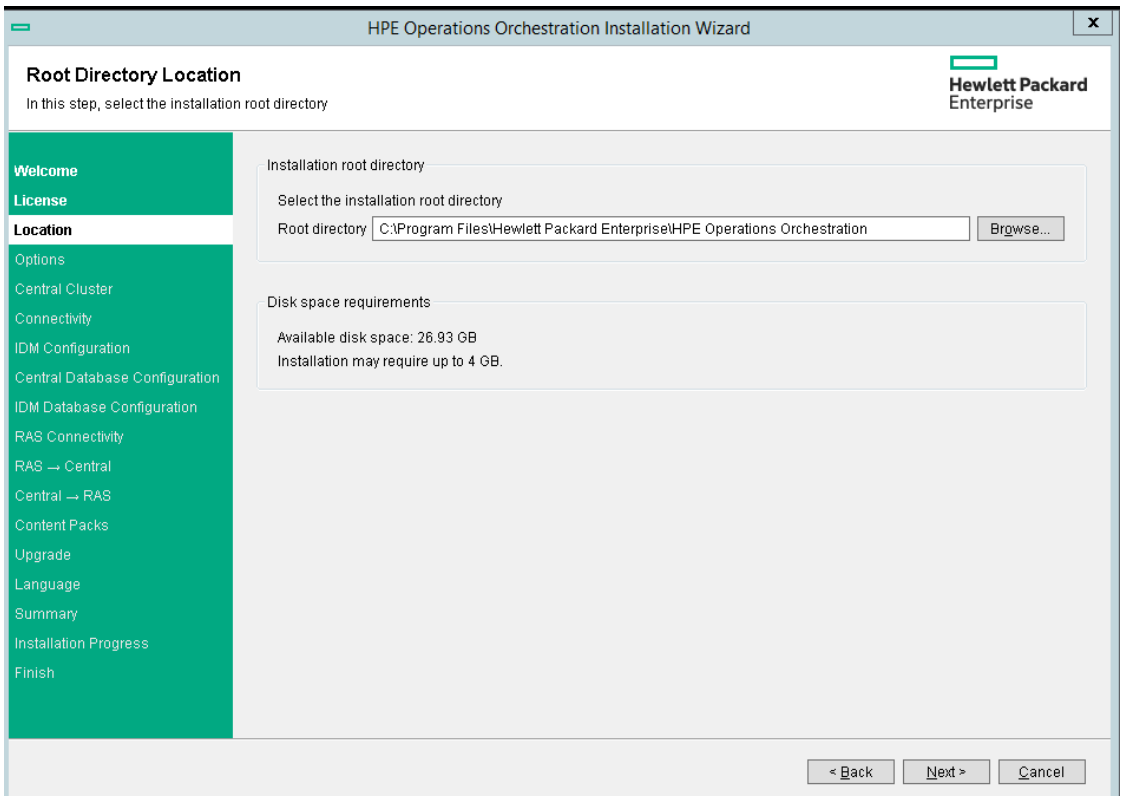
Back to the flowchart

Enter the Installation Location or Use the Default Location

1. In the **Location** step, select the location for the installation root directory, and then click **Next**.

   The default path is `C:\Program Files\Hewlett-Packard Enterprise\HPE Operations Orchestration`. Valid characters for the installation path include English letters, digits, spaces, hyphens (-) and underscores (_).

   If the directory does not exist, the directory will be created automatically. You are prompted to confirm the creation of the new location.

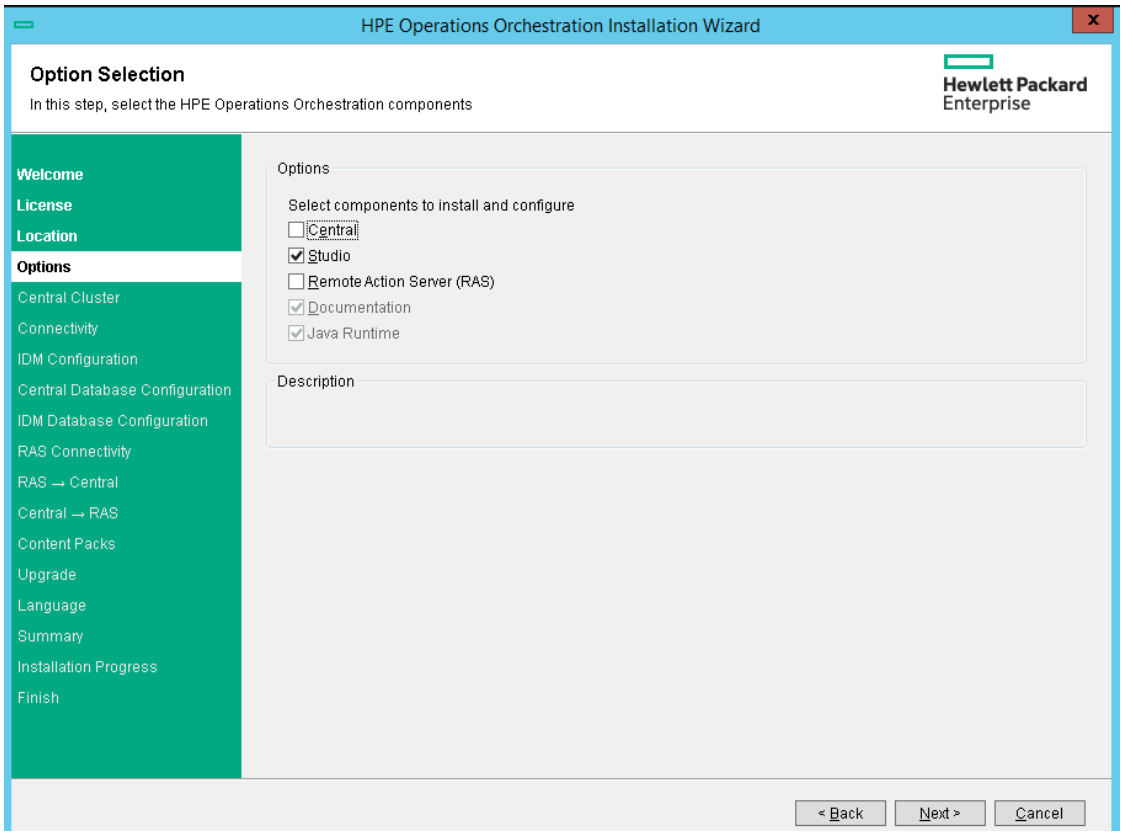


2. Click **Next**.

Back to the flowchart

Choose All the Installation Components

1. In the **Options** page, select the **Studio** check box.



2. Click **Next**.

Back to the flowchart

Select Content Packs for Studio Deployment

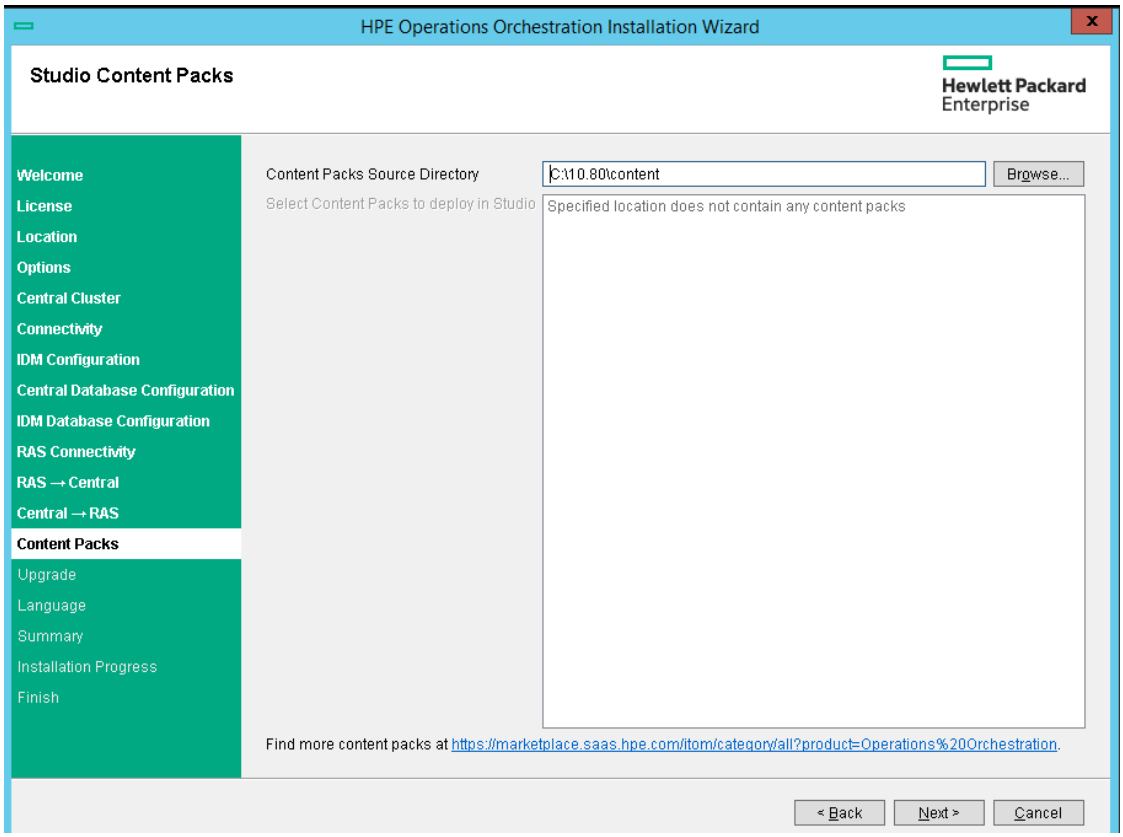
In the **Content Packs** page, you can import one or more content packs.

1. Browse to the location where the content packs are located, and then click **OK**.

   The available content packs located in the selected folder appear in the list.

   > **Note:** The installation folder includes the released content packs.

2. Select the content pack (or packs) that you want to import, and then click **Next**.



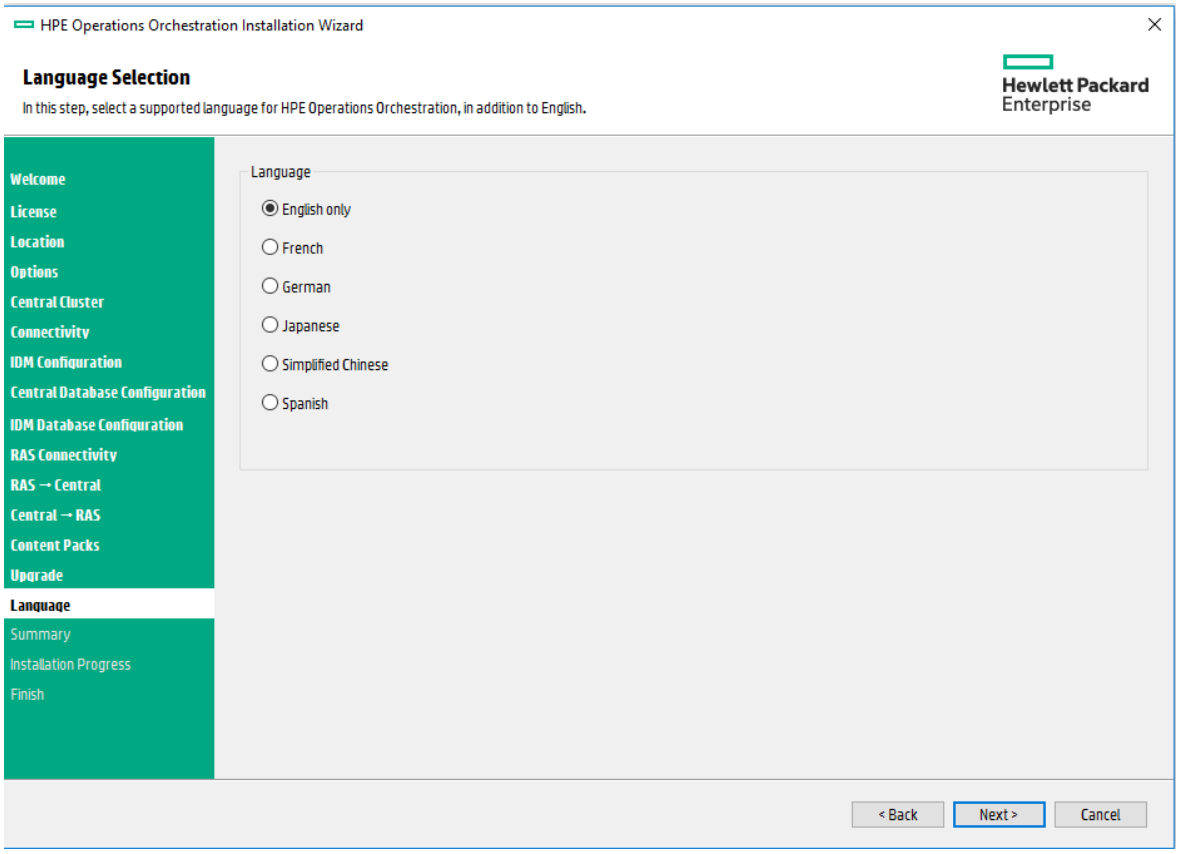
> **Note:** The content packs in the image above are just an example. Select the appropriate content packs.
>
> You can download additional and updated content packs on ITOM Marketplace, using the link in the lower part of the wizard.

Back to the flowchart

Select the Language

In the **Language** step, select a supported language for Operations Orchestration, in addition to English, and then click **Next**.This language support will be used for the Studio UI.

You can change the language support choice after installation, by editing the **Studio.properties** file, located in the installation directory under and **studio/conf**.



Back to the flowchart

Review Settings and Install

1. The **Summary** page displays the installation and configuration settings that you selected and entered in the wizard. Check that the settings are correct. If you want to correct one of the items, click **Back**.
2. Click **Install**. The installation begins, and the wizard displays a check mark next to each successfully installed item on the **Progress** page. When the installation is complete, click **Next**.

   > **Note:** If there is a problem with one of the installation or configured items, the installation attempts to continue with the rest of the items regardless of that error. Check the **installer.log** file (the default location is **C:\HPE\oo**) to check for errors.

3. (Optional) In the **Finish** page, select **Launch Studio** to start Studio.
4. Click **Finish** to close the Installation and Configuration wizard.

Back to the flowchart

Installation is Complete

Studio is now installed and menu shortcuts are created on your system.

You can also start **Studio** from the Windows **Start** menu:

From the Windows **Start** menu, select **All Programs** > **HPE Operations Orchestration** > **Studio**.

> **Note:** The minimum screen resolution for Studio is 1280x1024.

After installing Studio, in order to use the Studio Git integration feature, you must install the Git client version 2.9.2.

1. Download the Git client from the following URL: https://github.com/git-for-windows/git/releases/download/v2.9.2.windows.1/Git-2.9.2-64-bit.exe.
2. Save the Git client to **<oo_installation_folder>/studio/Git**, so that the **bin** folder is directly under **<oo_installation_folder>/studio/Git**. In the Git installation wizard, use the default options.

Alternatively, if you already have a Git client installation on your local disk, point Studio to use that Git installation by performing the following steps:

1. Close Studio.
2. Go to the user home folder **C:\Users\<user>\.oo** (the Studio workspace location) and locate the **Studio.properties** file.
3. Modify the **Studio.properties** file by adding the following property at the end of the file:

   ```
   studio.git.installation.location=<git_installation_folder>
   ```

   For example:

   ```
   studio.git.installation.location=C:/Program Files/Git
   ```

   The **bin** folder should be directly under **C:/Program Files/Git**. Note that **/** should be used as a path separator.
4. Save the **Studio.properties** file and start Studio.

> **Note:** If you opted for this second alternative, you need to consider the following:
>
> If you are using multiple workspaces and you want the Git location property to be added in each new workspace, you should edit the template properties file located in **Studio\conf\studio.properties.template**. Otherwise, each time you switch to a new workspace, you will have to set the Git location in the new workspace in the **.oo\Studio.properties** file.

If you have another version of the Git client installed, note that you must use version 2.9.2 of Git with Studio. This is the version that was validated with Studio. While other versions might still work correctly, they are not officially supported.

Installing Operations Orchestration RAS Using the Installation Wizard

> This section is applicable to both Standalone and Containerized installation.

This section describes how to perform a clean installation of an Operations Orchestration RAS.

Start the Operations Orchestration RAS Installation

1. Use the RAS installer available in the software entitlement set of the suite you are using. The available installer files are `installer-win64-ras.exe`and `./installer-linux64-ras.bin` for windows and linux respectively.

   Download the ZIP file from "software entitlement set" the HPE SSO Portal and extract it into a local drive on your computer.

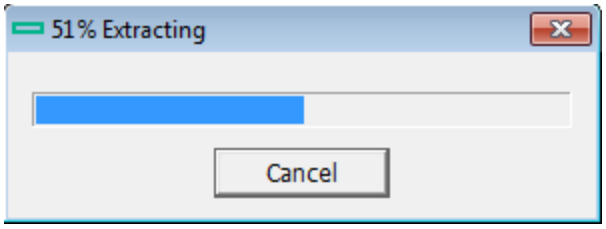
2. To start the installer:

   a. On Windows: Double-Click the `installer-win64-ras.exe` installation file.

   b. On Linux: Run the following command from the command line.
   `./installer-linux64-ras.bin -s silent.properties`
   Where, the `silent.properties` is a file which contains the required settings for OO RAS installation.

   Go to "References" on page 57 to see a sample `silent.properties` file.

3. After you start the installer, the installation package is extracted, and the **Operations Orchestration Installation and Configuration Wizard** automatically opens. Click **Next**.



4. In the **License** page, select **I Agree**, and then click **Next**.

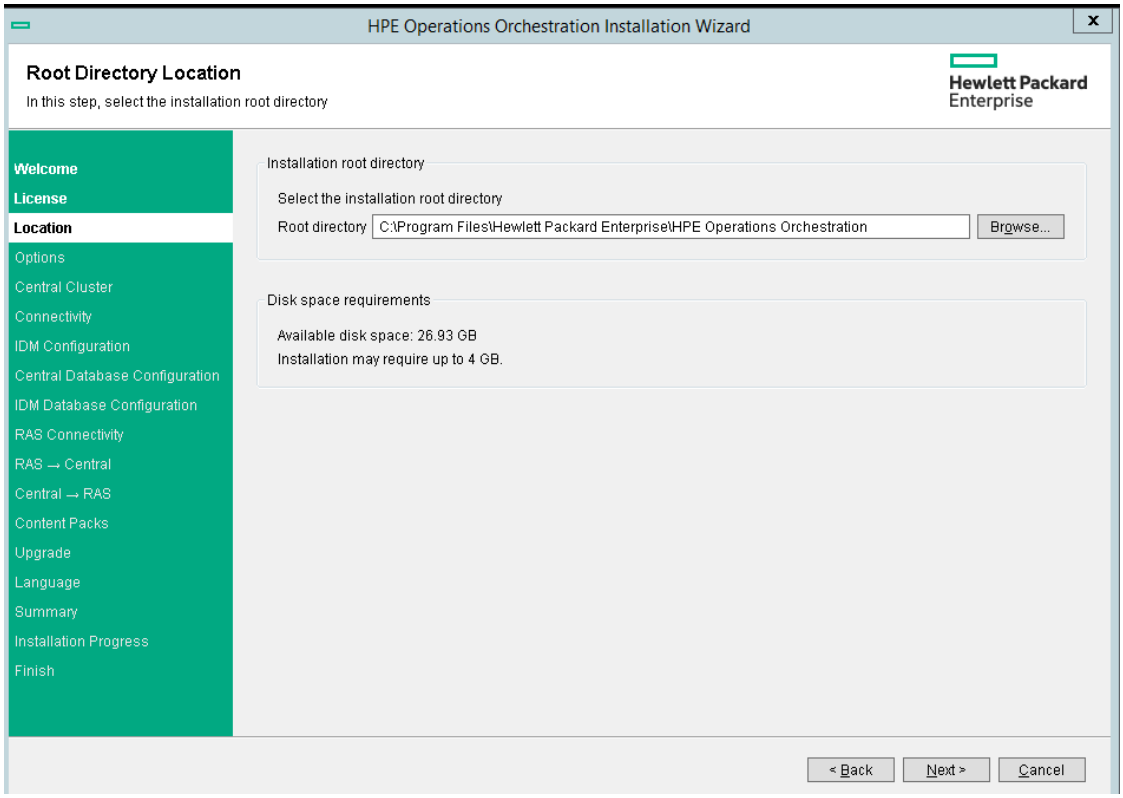
Back to the flowchart

Enter the Installation Location or Use the Default Location

1. In the **Location** page, select the location for the installation root directory.

   If the directory does not exist, the directory is created automatically. You are prompted to confirm the creation of the new location.

   > **Note:** Valid characters for the installation path are English letters, digits, spaces, hyphens (-) and underscores (_).
   >
   > The default path is `C:\Program Files\Hewlett-Packard Enterprise\HPE Operations Orchestration` for Windows and is `/opt/hpe/oo` for Linux.



2. Click **Next**.

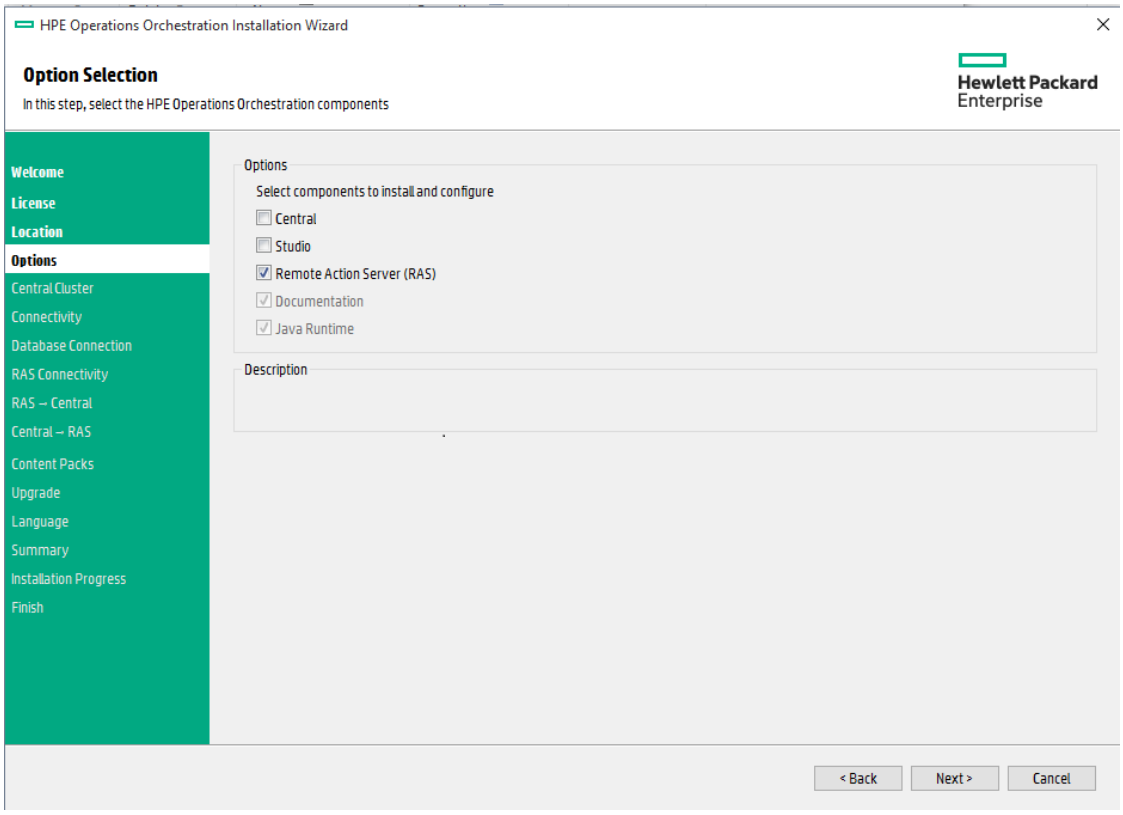
Back to the flowchart

Choose the Installation Components

> f you use `installer-win64-ras.exe` or `installer-linux64-ras.bin` file to install standalone RAS, then the options for other components are grayed out on **Option Selection**

screen. You are allowed to select only the **Remote Action Server (RAS)** option.

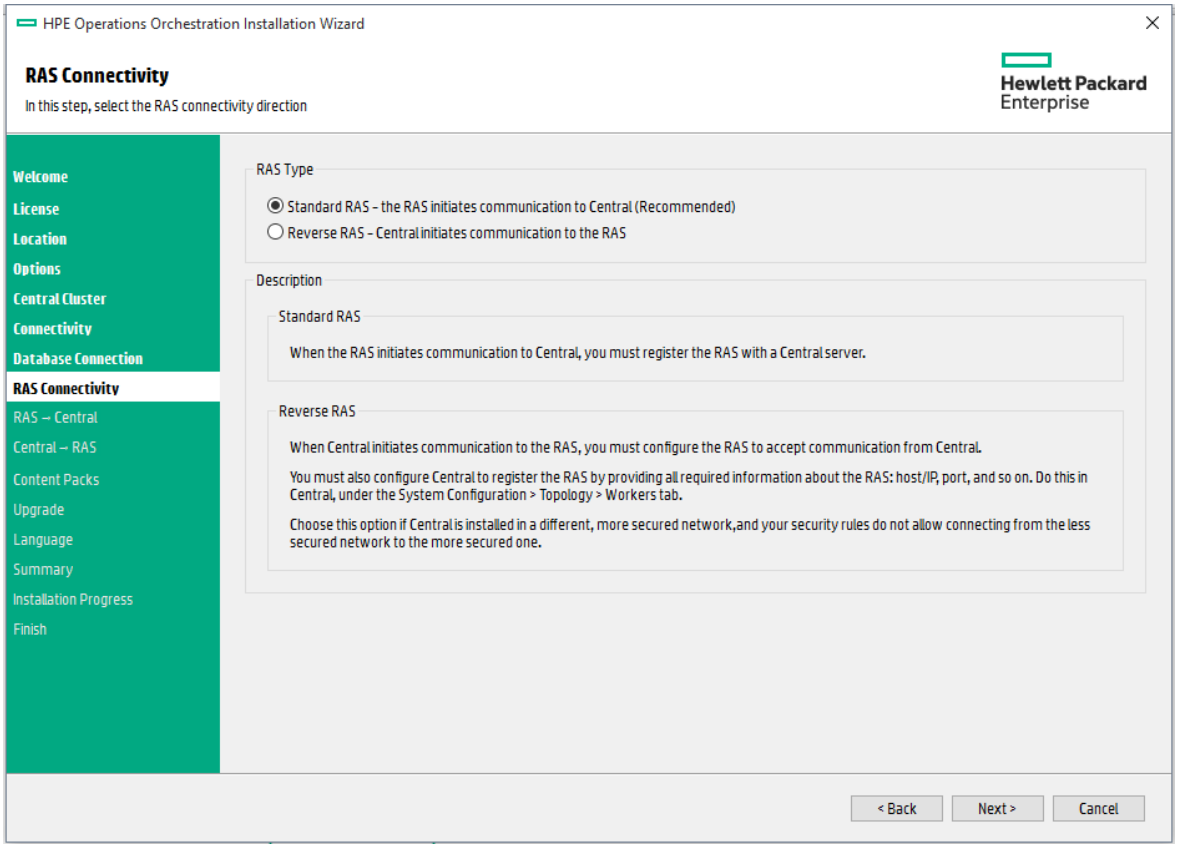
1. In the **Options** page, select the **Remote Access Server (RAS)** check box.



2. Click **Next**.

Back to the flowchart

Select the RAS connectivity direction



Choose between one of the following options:

- **Standard RAS - RAS initiates communication to Central** - this is the simplest option and is recommended if your security rules permit it.
- **Reverse RAS - Central initiates communication to RAS** - choose this option if Central is installed in a different, more secured network, and your security rules do not allow connecting from the less secured network to the more secured one.

  You will need to configure the RAS to accept connection from Central. When the RAS starts up, it will be idle, waiting for Central to initiate connection.

Back to the flowchart

RAS -> Central: Enter the RAS registration settings

This step follows if you selected **Standard RAS - RAS initiates communication to Central**.

> **Note:** If you are installing RAS and Central at the same time, this page does not appear, because the RAS is automatically registered to the Central that is being installed at the same time.

1. In the **RAS -> Central** page, enter, in the **Central URL** box, enter the properties and location of the Central.

   Make sure to use the FQDN (Fully Qualified Domain Name) for the Central URL.

   If you want to use IPv6, put the IPv6 address in brackets, for example, [3fff::20]. Otherwise, errors will occur.

   > **Note:** If Central is set up with HTTPS, make sure to enter the hostname *exactly* as specified in Central's TLS certificate.

2. (Optional) Select the **Central user capable of registering a RAS** check box and enter the user name and password of this user.

   If relevant, add the LDAP domain using the following conventions:

   - domain\username
   - username@domain

3. (Optional) Select the **HTTP proxy definition for connecting to the Central** and enter the HTTP proxy definition.
4. Click **Test Connection**.

   > **Note:** If you test the connection to a Central with a custom CA certificate without providing the certificate to the RAS, a java.lang.RuntimeException error message will appear.

   - If the connection test is successful, continue.
   - If the connection test is not successful, review the settings that you entered in steps 1 - 3 above.

5. When you installed Central, if you provided a CA certificate for Central, you must provide the root CA certificate for the RAS. This certificate will be imported to the RAS TrustStore:

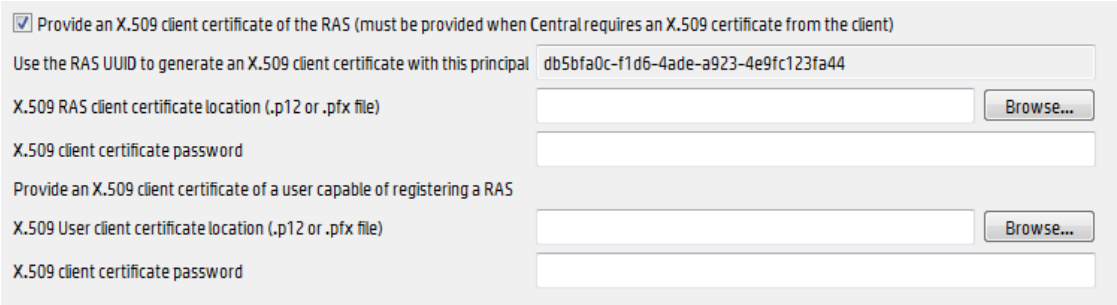
   a. Select the **Supply the CA root certificate of Central** check box.

   b. Click **Browse** to select the relevant CA root certificate.

   If the default certificates were used in Central, you should leave this check box cleared, to automatically use the self-signed certificate.

   For more information about using TLS certificates, see the *Operations OrchestrationSecuring and Hardening Operations OrchestrationGuide*.

6. If Central requires an X.509 certificate from the client, follow these steps (you may need to scroll down to see all the fields):



a. Click the **Provide an X.509 client certificate of the RAS** check box.

   A UUID for the RAS is automatically generated.

b. Create the client certificate using this RAS UUID. The client certificate must be in PKCS format and must be with a **.pfx** or **.p12** extension.

c. Click **Browse** to select the X.509 client certificate that you created.

d. Enter the password of the X.509 client certificate that you created.

e. Click **Browse** to select the client certificate of a user capable of registering a RAS.

f. Enter the password for the user capable of registering a RAS.

7. Click **Next**.

Back to the flowchart

Central -> RAS: Configure RAS ports and TLS properties

This step follows if you selected **Reverse RAS - Central initiates communication to RAS**.

1. In the **Central -> RAS** page, enter a shared secret, and enter it again to confirm.

   When Central is configured to register this RAS, this secret will need to be entered, in order for Central to connect to the RAS.

   The shared secret must conform to the following rules:

   - Minimal length of 8 characters
   - Contain at least one upper case character
   - Contain at least one lower case character
   - Contain at least one number

2. In the **RAS listening address** box, enter the FQDN or IP of the RAS server.

   By default, this is populated with the IP/FQDN (based on the selected protocol).

3. Enter the port on which the RAS server will listen for the Central connection.
4. Click **Test port availability**. If the ports are available, a **Success** check mark appears.

   If you encounter an error, adjust the ports accordingly and try again.
5. (Recommended) Select **Supply a secure TLS certificate**.

   This step is recommended, for security reasons. If you do not select a secure TLS certificate, Operations Orchestration will generate and use a self-signed certificate, which will be exported to the **<RAS>/var/security** folder.
6. If you selected **Supply a secure TLS certificate**, click **Browse** to specify the location of the RAS TLS certificate.
7. Enter the certificate's password and enter it again for confirmation.
8. Click **Next**.

Back to the flowchart

Configure Central to register the Reverse RAS

If you selected **Reverse RAS - Central initiates communication to RAS**, you must also configure Central to register the RAS, by providing all required information about the RAS: host/IP, port, and so on.

You need to do this in Central, under the **System Configuration** > **Topology** > **Workers** tab. Once the RAS is registered, Central opens the connection to the RAS.

> **Note:** If the protocol is HTTPS, make sure that the root certificate from the reverse RAS has been added to the Central's client.truststore before attempting to register the worker in the Central UI. It is not required to restart Central after importing the certificate.

> **Note:** If you selected Reverse RAS, the installation process creates a file named **ras-connectivity.properties** under **<installation-directory>\ras\conf**.
>
> . This file includes the following information:
>
> - protocol type: WS/WSS
> - listen address: FQDN/IP
> - listen port: <integer>
> - reverse RAS flag: true/false (The RAS uses this flag to define the mode to use upon startup: regular RAS or reverse RAS)
> - hashed shared secret

For more information, see "Setting Up Topology – Workers and RASes" in the Operations Orchestration *Central User Guide*.

Back to the flowchart

Review Settings and Install

A summary of the installation is displayed.

Review the settings and click **Install**.

Back to the flowchart

Installation is Complete

Click **Finish** to complete the installation.

References

Sample silent.properties file

> You can uncomment a line by removing # in the starting of a line.

```
########################################

####

#### General Properties

####

### Root directory of the installation

# root.dir=

# On Windows, the path must be with / or with \\

# Example (Windows): root.dir=c:/Program Files/Hewlett-Packard/HP Operations Orchestration

# Example (Linux): root.dir=/usr/local/hp/oo

### What to install

# install.java=

# Valid values: true, false

# Default: true

# This is required. You should only set this to false if Java Runtime has already been installed in the target directory.

# install.ras=
```

```
# Valid values: true, false

# Default: false

# install.central=

# Valid values: true, false

# Default: true

# install.studio=

# Valid values: true, false

# Default: false

# install.docs=

# Valid values: true, false

# Default: true

### Central server ports

# http.port=

# Default: 8080

# https.port=

# Default: 8443

### HTTP port access

# http.port.access=enable

# Options: enable (HTTP access is enabled)

# Options: disable (HTTP access is disabled)

# Default: http.port.access=enable

# HP recommends to disable the HTTP port and to use a TLS certificate for security
reasons.

### Whether to start Central after the installation

# should.start.central=

# Valid values: true, false

# If you are configuring HP OO to be compliant with FIPS 140-2, this must be set to
false.

# If you are installing a new Central in cluster mode and the installer version is
older

# than the current Central, this must be set to false.

# If you are upgrading from 9.x OR installing a RAS together with Central, Central
will be
```

```
# started, regardless of how this property is set.

### Select a supported language for HP Operations Orchestration, in addition to
English.

# language=

# Valid values: en, fr, de, ja, es, ch

# Default: en

# This configures the language for Central and Studio in the Studio.properties and
central-wrapper.conf files.

# For Central, this also changes the database schema language for SQL Server.

##########################################

####

#### IDM configuration

####

### Whether to install or connect to an IDM service

# idm.mode=

# Valid values: native, connect, create.

# Default: native

# native: use OO built-in authentication

# connect: connects to an existing IDM service

# create: installs the IDM service.

###

### Properties relevant only for idm.mode=create

### This option installs the IDM service along with OO Central.

###


# idm.configuration.internal.password=

# The password for the IDM super-user account, the super user in IDM is named
'admin' and is used by oo to communicate with the IDM service.

# idm.configuration.signing.key=

# The IDM configuration signing key. The signing key should be at least 32
characters. It must contain lower case, upper case and numeric characters.

# idmExportConfigurationToFile=

# Boolean value specifying whether to export IDM configurations to a file.
```

```
# Possible values: true, false.

# Default value: false

# idmExportFilePath=

# Absolute path to the export file location including the file name.

# On Windows, the path must be with / or with \\

# Example (Windows): idmExportFilePath=c:/Program Files/Hewlett-Packard/idm-saved-
configurations.txt

# Example (Linux): idmExportFilePath=/usr/local/hp/idm-saved-configurations.txt

# idmOverwriteExportFile=

# Boolean value specifying whether to override an existing file.

# Possible values: true, false.

# Default value: false

# idm.configuration.oo.admin.password=

# ooadmin user password, this is the password for the user with ADMINISTRATOR role
for OO Central.

# idm.configuration.oo.promoter.password=

# oopromoter user password, this is the password for the user with PROMOTER role,
can access the Content Management workspace and the Run Management workspace.

# idm.configuration.oo.system.admin.password=

# oosystemadmin user password, this is the password for the user with SYSTEM_ADMIN
role, can access the System Configuration workspace and the Run Management
workspace.

# idm.configuration.oo.end.user.password=

# ooenduser user password, this is the password for the user with END_USER role,
can only access the Run Management workspace.

# idm.configuration.oo.everybody.password=

# ooeverybody user password, this is the password for the user with EVERYBODY role,
can only access the Run Management workspace.

###

### Properties relevant only for idm.mode=connect

### This option connects OO Central to an existing IDM service.

###

# idm.configuration.url=

# IDM service url, format <http or https>://<HOSTNAME>:<PORT>/idm-service
```

```
# idm.configuration.username=

# The IDM transport username which OO will use in order to get the authentication
token from IDM service.

# Default value: idmTransportUser

# idm.configuration.password=

# The IDM transport username's password.

# idm.configuration.signing.key=

# The IDM configuration signing key. The signing key should be at least 32
characters. It must contain lower case, upper case and numeric characters.

# idm.configuration.oo.central.tenant=

# The name of the tenant/organization that must exist in IDM.

# Default value: OO_Central

# idm.configuration.internal.username=

# This is the IDM super-user account which will be created in IDM.

# OO Central will use this account in order to communicate with IDM service.

# idm.configuration.internal.password=

# The password for the IDM super-user account.

########################################

####

#### Properties Relevant to the First Installed Central in a Cluster, or to a
Standalone Central

####

####### Central server database properties

### Define the database type

# db.type=

# Valid values: oracle, postgresql, mysql, mssql, h2, and other.

# Default value: h2

# For db.type=mysql, db.driver.location MUST be set to the path of a MySQL JDBC
driver (a JAR

# file). It is also available for db.type=other.

# For db.type=H2, this uses an H2 local database. This should not be used for
production.
```

```
# For db.type=other, use to enable advanced features in supported databases. If you
select

# other, you can only use a database type that is supported for use with HP OO. See
the

# System Requirements for more information.

### Define the database driver

# db.driver=

# Resolved automatically from db.type, but can be overridden.

# Linkage: If db.type is other, this property is required.

### Define the location of the database JDBC driver

# db.driver.location=

# Linkage: Required when db.type=mysql or db.type=other. Required for mySQL even
when adding a node to a cluster.

# Example: db.driver.location=c:/tmp/mydriver.jar

# Note: This path is an example only. There is no need to create a tmp directory.

### Define the database JDBC URL

# db.url=

# This is optional. Set this value if you want advanced features supported by the
driver.

# Linkage: If you set this property, the db.host, db.port, db.name and
db.service.name properties are ignored.

# MySQL example: db.url=jdbc:mysql://<host>:<port>/<db.name>

# Oracle example with SID: db.url=jdbc:oracle:thin:@<host>:<port>:<sid>

# Oracle example with service name:
db.url=jdbc:oracle:thin:@//<host>:<port>/<service.name>

# PostgreSQL example: db.url=jdbc:postgresql://<host>:<port>/<db.name>

# MS Sql example: db.url=jdbc:jtds:sqlserver://<host>:<port>/<db.name>

### Define the database host name

# db.host=

# Linkage: This property is ignored when db.url is used.

### Define the database port

# db.port=

# Linkage: This property is ignored when db.url is used.
```

```
### Define the database name or SID (depending on the type of database)

# db.name=

# Linkage: This property is ignored when db.url is used.

# Example: db.name=ORCL

# You cannot use special characters for the database name or SID, except the
underscore (_).

# You can enter up to 30 characters for the database name or SID.

### Define the name of the database user

# db.username=

# This user name is required when you use the option to create a database.

# The username is required also when connecting to an existing schema, the
difference is

# that it’s not being created during the installation.

# The user name is created by the installer and eventually used by HP OO.

# Example: db.username=joe

# In Oracle, do not use SYS, SYSTEM, or other administrative account credentials.

# In Microsoft SQL Server, do not use sa or other administrative account
credentials.

# In PostgreSQL, do not use postgres credentials.

# PostgreSQL database names are case-sensitive.

### Define the password of the database user

# db.password=

# This password is required when you use the option to create a database.

# The password is required also when connecting to an existing schema, the
difference is

# that it’s not being created during the installation.

# The password is created by the installer and eventually used by HP OO.

# Example: db.password=pass

# In Oracle, do not use SYS, SYSTEM, or other administrative account credentials.

# In Microsoft SQL Server, do not use sa or other administrative account
credentials.

# In PostgreSQL, do not use postgres credentials.

### Specify whether to create the database schema during installation
```

```
# To create the database schema you must provide the admin user credentials. This
is a database user capable of

# creating a schema or database. Usually, this is a DBA user or a system user

# db.create-schema=

# Valid values: true, false

# Default: false

### Define the admin user of the database

# db.admin.username=

# Used to create a schema/database/user

# Example: db.admin.username=postgres

### Define the database admin user password

# db.admin.password=

# Used to create a schema/database/user

# Example: db.admin.password=manager

### Define the default tablespace name for the created user (Oracle only)

# db.tablespace=

# Example: db.tablespace=USERS

# Linkage: Only used when creating a schema (user) in an Oracle database

### Define the default temporary tablespace name (Oracle only)

# db.temp.tablespace=

# Example: db.temp.tablespace=TEMP

# Linkage: Only used when creating a schema (user) in an Oracle database

### Define the database connection type (Oracle only)

# Valid values: sid, service

# Default value: sid

# db.oracle.connection.type=

# Example: db.oracle.connection.type=sid

# Linkage: Only used when setting up an Oracle database

### Define the database service name (Oracle only)

# db.service.name=

# Example: db.service.name=orcl_name
```

```
# Linkage: Only used when db.oracle.connection.type=service

### Define the database SID (Oracle only)

# db.name=

# Example: db.name=orcl_sid

# Linkage: Only used when db.oracle.connection.type=sid

####### IDM server database properties

# The below configuration parameters are required only when idm.mode=create, and
represent the database to which IDM service will be connected to.

# The database schema must exist prior to the installation and the schema name
cannot be the same as the OO Central's schema name.

# Important note: IDM connects to the same database host as Central. This means
that the database type, hostname and port will be inherited from Central's database
configuration.


### Define the database username

# idm.db.username=

# This is the username that IDM will use to connect to it's existing schema.

# Example: idm.db.username=idmServer

# In Oracle, do not use SYS, SYSTEM, or other administrative account credentials.

# In Microsoft SQL Server, do not use sa or other administrative account
credentials.

# In PostgreSQL, do not use postgres credentials.

# PostgreSQL database names are case-sensitive.

### Define the database name or SID (depending on the type of database)

# idm.db.name=

# Example: idm.db.name=ORCL

# You cannot use special characters for the database name or SID, except the
underscore (_).

# You can enter up to 30 characters for the database name or SID.

### Define the password of the database user

# idm.db.password=

# Example: idm.db.password=pass

# In Oracle, do not use SYS, SYSTEM, or other administrative account credentials.
```

```
# In Microsoft SQL Server, do not use sa or other administrative account
credentials.

# In PostgreSQL, do not use postgres credentials.

### Define the database service name (Oracle only)

# idm.db.service.name=

# Example: idm.db.service.name=orcl_service_name

# Linkage: Only used when the database is configured to connect to an Oracle
database configured with a service name.

# If Central is configured to connect to an Oracle

# Default value: sid

# Required only when the Oracle database configuration is with  service name
instead of sid, if the parameter is not supplied the oracle configuration will be
with sid.

########################################

####

#### Upgrading from HP OO 9

####

#### The Upgrade Properties are Relevant to the First Installed Central in a
Cluster, or to a Standalone Central

# Note; When you are upgrading from a remote 9.x Central that has localhost as the
database in the

# Central.properties file using a silent installation, installation and upgrade do
not complete

# successfully. This problem does not exist for wizard installations.

### Specify Whether an upgrade from HP OO 9.x should be performed.

# upgrade.required=

# Valid values: true, false

# Default: false

### Define the upgrade source from where to perform the upgrade

# upgrade.source=

# Valid values: files, directory, database

# files: You need to provide the files from the 9.x installation regardless of
whether it is installed on the same computer as 10.x or not.
```

```
# The files are located on 9.x machine under the path <9.x installation
folder>/Central/conf/ and can be copied on the 10.x installation machine or on a
shared resource.

# directory: You need to provide the 9.x installation directory. This can be on the
same computer or shared (SMB, NFS) and mounted on the 10.x computer.

# database: You only need to provide the 9.x database properties

# Example: upgrade.source=files

### Define the location of the Central properties, in an upgrade

# upgrade.central.properties.location=

# Linkage: This needs to specified if upgrade.source=files

# This location should point to the mounted 9.x installation folder or where these
files where copied from 9.x

# Example: upgrade.central.properties.location=<shared path>/Central.properties

### Define the location of the central-secured.properties, in an upgrade

# upgrade.central-secure.properties.location=

# Linkage: This needs to specified if upgrade.source=files

# This location should point to the mounted 9.x installation folder or where these
files where copied from 9.x

# Example: upgrade.central-secure.properties.location=<shared path>/central-
secured.properties


### Define the 9.x installation home directory, in an upgrade

# upgrade.9x.home.location=

# Linkage: This needs to specified if upgrade.source=directory

# Example: upgrade.9x.home.location=c:/Program Files/Hewlett-Packard/Operations
Orchestration

### Define the 9.x database type, in an upgrade

# upgrade.db.type=

# Valid values: oracle, mssql, or mysql

# Linkage: This needs to specified if upgrade.source=database

# Required if HP OO 9.x is running over a MySQL database (regardless of

# upgrade.source).Otherwise, not needed.

# Example: upgrade.db.type=mysql
```

```
### Define the 9.x database host name, in an upgrade
# upgrade.db.host=
# Linkage: This needs to specified if upgrade.source=database
# Example: upgrade.db.host=ninexdb
### Define the 9.x database port number, in an upgrade
# upgrade.db.port=
# Linkage: This needs to specified if upgrade.source=database
# Example:upgrade.db.port=1521

### Define the 9.x database name/SID, in an upgrade
# upgrade.db.name=
# Linkage: This needs to specified if upgrade.source=database
# Example:upgrade.db.name=ORCL
### Define the 9.x database user name, in an upgrade
# upgrade.db.username=
# Linkage: This needs to specified if upgrade.source=database
### Define the 9.x database password, in an upgrade
# upgrade.db.password=
# Linkage: This needs to specified if upgrade.source=database

### Specify the location of the JDBC driver, in an upgrade
# upgrade.db.driver.location=
# Linkage: Required if HP OO 9.x is running over a MySQL database (regardless of
# upgrade.source). Otherwise, not needed
# Exampe: upgrade.db.driver.location=C:/tmp/mysql-connector-java-5.1.21.jar
########################################
####
#### Properties Relevant to a Standalone Central, RAS, Studio
####
### Define whether the SSl certificate is user-provided or self-signed
# ssl.certificate.type=
```

```
# Valid values: self-signed, user-provided

# Linkage: If you chose to set ssl.certificate.type to be user-provided, you must
also set a

# value for ssl.user-provided-root-certificate.location

# Example: ssl.certificate.type=self-signed

### Specify the location of the user-provided keystore with the server certificate

# ssl.user-keystore.location=

# This must be in PKCS12 format

# On  Windows, the path can use either / or \\

# Example: ssl.user-keystore.location=c:/tmp/certificate.p12/pfx

### Define the password for the user-provided keystore with service certificate

# ssl.user-keystore.password=

### Specify the location of the root certificate to be imported.

# ssl.user-provided-root-certificate.location=

# Needed only if Central was installed with different certificates than self-
signed.

# The root certificate must be in .cer or .crt format

# Linkage: If you chose to set ssl.certificate.type to be user-provided for
Central, and if you

# chose to install both Central and RAS, you must set a

# value for ssl.user-provided-root-certificate.location

# Example: ssl.user-provided-root-certificate.location=c:/tmp/my.cer

# Example: ssl.user-provided-root-certificate.location=c:\\tmp\\my.cer

########################################

####

#### Properties Relevant to a Central Node in a Cluster, But Not to the First
Installed Central

####

#### Determine if this is a cluster installation

# central.cluster=

# Valid values: true, false

# Default: false

#### Specify the absolute path of the database.properties file
```

```
# central.cluster.database.properties=

# Absolute path of the database.properties file on the local machine, copied from
an existing node

# in HP OO 10.x, from <10.x installation>/central/conf.

# Example:
central.cluster.database.properties=C:/<installation>/central/conf/database.propert
ies

#### Specify the absolute path of the encryption.properties file

# central.cluster.encryption.properties=

# Absolute path of the encryption.properties file on the local machine, copied from
an existing node

# in HP OO 10.x, from <10.x installation>/central/var/security

#
Example:central.cluster.encryption.properties=C:/<installation>/central/var/securit
y/encryption.properties

#### Specify the absolute path of the encryption_repository

# central.cluster.encryption_repository=

# Absolute path of the encryption_repository file on the local machine, copied from
an existing node

# in HP OO 10.x, from <10.x installation>/central/var/security

# Example: central.cluster.encryption_
repository=C:/<installation>/central/var/security/encryption_repository

# db.driver.location=

# When using a MySQL database (in either HP OO 10 or in an upgraded HP OO 9), it

# would normally be required to set this property. However, when installing a

# cluster node, this property is ignored due to an issue in the 10.00 installer.

# Therefore, you must manually copy the file to <installation>/central/lib and

# <installation>/central/tomcat/lib after the installation, then start the node.

# db.driver.location=C:/Users/admin/Desktop/mysql-connector-java-5.1.21.jar

### Whether to start Central after the installation

# should.start.central=

# Valid values: true, false

# If you are installing a new Central in cluster mode and the installer version is
older
```

```
# than the current Central, this must be set to false.

########################################

####

#### Installing a  standard RAS

####

#### Root directory of the installation:

# root.dir=C:/Program Files/Hewlett-Packard/HP Operations Orchestration

#### What to install:

# install.java=true

# install.central=false

# install.ras=true

# install.studio=false

#### Define the Central connection properties - used to connect the RAS to the
central

# central.url=

# In the formats: http://<server-FQDN> or <IP address>:<HTTP_PORT>/oo

# Example: central.url=http://16.59.62.205:8293/oo

# If you are using a cluster, this should be the load balancer's URL:

# central.url=https://74.125.225.240:8443/oo

#### Define whether or not access to Central requires an HTTP proxy

# central.proxy=

# Valid values: no, manual

# Default: no

### Define the HTTP proxy host name for connecting to Central.

# central.proxy-hostname=

# Example: proxy-hostname=myhost

### Define the HTTP proxy port for connecting to Central

# central.proxy-port=

# central.proxy-port=880

### Define the HTTP proxy user name for connecting to Central, if proxy requires
authentication.

# central.proxy-username=
```

```
### Define the HTTP proxy password for connecting to Central, if needed.
# central.proxy-password=
### Specify whether the Central is password protected
# central.secured=
# valid values for central.secured: true, false
# Default: true
### Define the Central user name that has MANAGE_TOPOLOGY permission.
# central.username=
# Example: central.username=oouser
### Define the Central user's password
# central.password=
# Example: central.password=oopass
### Define whether the RAS requires a SSL user-provided certificate to register
# ssl.certificate.type=
# Valid values: self-signed, user-provided
# Linkage: If your Central was installed with a user provided certificate
# set this value to user-provided and also provide a
# value for ssl.user-provided-root-certificate.location
# Example: ssl.certificate.type=self-signed
### Specify the location of the root certificate to be imported.
# ssl.user-provided-root-certificate.location=
# Needed only if Central was installed with different certificates than self-
signed.
# The root certificate must be in .cer or .crt format
# Linkage: If you chose to set ssl.certificate.type to be user-provided for
Central, and if you
# chose to install both Central and RAS, you must set a
# value for ssl.user-provided-root-certificate.location
# Example: ssl.user-provided-root-certificate.location=c:/tmp/my.cer
# Example: ssl.user-provided-root-certificate.location=c:\\tmp\\my.cer
### Specify whether the X.509 client certificate should be provided by the RAS to
Central
```

```
# ssl.client.certificate=

# Valid values: true, false

# Default: false

# This must be provided when Central requires an X.509 certificate from the client
as a part of the SSL handshake.

### Define the full path to the X.509 client certificate location of a user capable
of registering a RAS

# ssl.user.client.certificate.location=

# On Windows, the path must be with / or with \\



### Define the X.509 client certificate password

# ssl.user.client.certificate.password=

### Define the full path to the X.509 client certificate location

# ssl.user-provided-client-certificate.location=

# On Windows, the path must be with / or with \\

### Define the X.509 client certificate password

# ssl.client.certificate.password=

### Define the UUID of the RAS

# ssl.client.certificate.ras.uuid=

# If Central requires an X.509 client certificate, you need to generate it.

# The X.509 client certificate needs to have the principal name of the RAS, which
is

# the RAS UUID (see "Processing a Certificate Principal" in the HP OO System

# Security and Hardening Guide).

# This must be in the UUID format.

# You must generate the UUID and provide it here.

# Example of UUID format: c7fd89e1-d703-44a1-b067-732b8ebbfe23

### Define the connectivity direction of the RAS

### This determines whether the RAS initiates the connection to Central (standard
RAS)

### or whether the RAS waits for Central to initiate the connection (reverse RAS)

# register.ras=true
```

```
# Valid values: true, false

# true = standard RAS, false = reverse RAS

########################################

####

#### Installing a  reverse RAS

####

#### Root directory of the installation:

# root.dir=C:/Program Files/Hewlett-Packard/HP Operations Orchestration

#### What to install:

# install.java=true

# install.central=false

# install.ras=true

# install.studio=false

### Define the connectivity direction of the RAS

### This determines whether the RAS initiates the connection to Central (standard
RAS)

### or whether the RAS waits for Central to initiate the connection (reverse RAS)

# register.ras=false

# Valid values: true, false

# true = standard RAS, false = reverse RAS

# shared.secret=

# For a reverse RAS, enter the shared secret that will be used by Central, to
communicate with this RAS

# ras.server.address=

# Enter the IP address of the reverse RAS

# Example: ras.server.address=16.60.234.64

# ras.connectivity.protocol=

# Enter the protocol of the reverse RAS

# Valid values: HTTPS, HTTP

# Example: ras.connectivity.protocol=HTTPS

# ras.connectivity.central.initiates.https.port=

# Enter the https port number of the reverse RAS (if protocol == HTTPS)
```

```
# Example: ras.connectivity.central.initiates.https.port=8443

# ras.connectivity.central.initiates.http.port=

# Enter the http port number of the reverse RAS(if protocol == HTTP)

# Example: ras.connectivity.central.initiates.http.port=8080

### Define whether the SSl certificate is user-provided or self-signed

# ssl.certificate.type=

# Valid values: self-signed, user-provided

# Linkage: If you chose to set ssl.certificate.type to be user-provided, you must
also set a

# value for ssl.user-provided-root-certificate.location

# Example: ssl.certificate.type=self-signed

### Specify the location of the user-provided keystore with the server certificate

# ssl.user-keystore.location=

# This must be in PKCS12 format

# On  Windows, the path can use either / or \\

# Example: ssl.user-keystore.location=c:/tmp/certificate.p12/pfx

### Define the password for the user-provided keystore with service certificate

# ssl.user-keystore.password=

########################################

####

#### Studio properties

####

#### Root directory of the installation:

# root.dir=C:/Program Files/Hewlett-Packard/HP Operations Orchestration

#### What to install:

# install.java=true

# install.central=false

# install.ras=false

# install.studio=true

### Specify the content packs to be imported to Studio

# studio.content.packs=
```

```
# Optional - use this if you want to auto-import CPs on first Studio startup.

# Absolute paths to the needed CPs, separated by comma.

# Example: studio.content.packs=C:/tmp/oo10-base-cp-1.0.142.jar,C:/tmp/my-cp-
1.0.0.jar
```

Important Notes About Silent Installation

- Be careful not to put trailing spaces in your property values (especially when pasting). Otherwise, values that contain spaces at the end will not be read correctly and installation might fail.
- **Oracle**: Do not use `SYS`, `SYSTEM`, or other administrative account credentials in the **db.username**/**db.password** properties.
- **PostgreSQL**: Do not use **postgres** credentials in the **db.username**/**db.password** properties.

  > **Note:** PostgreSQL database names are case-sensitive.

- db.type=H2: This uses an H2 local database. This should not be used for production.
- db.type=other: Use to enable advanced features in supported databases. If you select **other**, you can only use a database type that is supported for use with Operations Orchestration. See the *Operations Orchestration System Requirements* for more information.
- Special characters, except the underscore (_), cannot be used for the database name or SID. In addition, you can enter up to 30 characters for the database name or SID.
- When you are upgrading from a remote 9.x Central that has localhost as the database in the **Central.properties** file using a silent installation, installation and upgrade do not complete successfully. This problem does not exist for wizard installations.
- All property values that contain a backslash ('\') in the **silent.properties** file need to be escaped (with a double-backslash instead of a single one).

  Places where this might be needed:

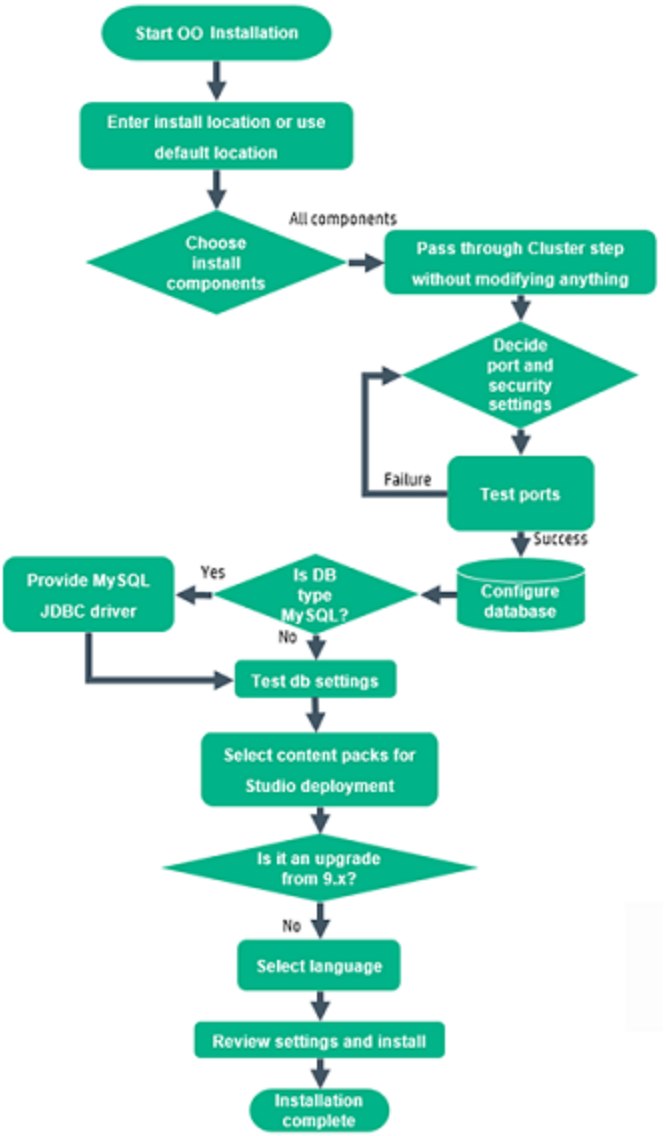
  - On Japanese environments, in all the paths given. In Japanese environments, the path separator is the Yen sign and it needs to be escaped. For example, `C:¥¥folder`
  - For RAS installations with a LDAP user given in form of 'domain\user'.
  - For a database user, if the database is set up with Windows system account authentication
  - For any other user that contains a backslash in the name

> There are some instances where the default values are different in a silent installation. For example, when installing with the wizard, by default the certificate is set to CA (user provided), while in a silent installation, this defaults to self-signed.

Installing All Operations Orchestration Components Using the Installation Wizard

> This section is applicable only if you install Operations Orchestration 10.80 in Standalone mode. This is not applicable if you install Operations Orchestration as a container as part of suite installation.

This section describes how to perform a clean installation of Operations Orchestration, including all components: Central, RAS, and Studio. Click each node on the map to jump to the relevant topic.



Note: Studio (the flow authoring tool) only works on Windows. So if you are installing Operations Orchestration on Linux, note that you will have to run the installer separately on Windows, in order to install Studio.

Start the Operations Orchestration Installation

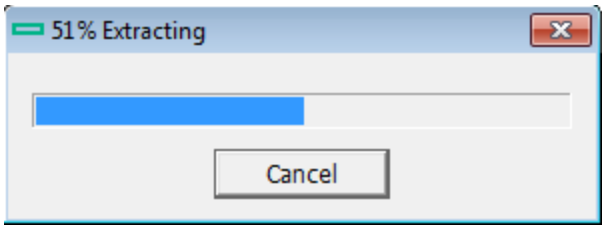
1. Download the ZIP file from the HPE SSO Portal and extract it into a local drive on your computer.
2. To start the installer:

- On Windows: Double-click the **installer-win64.exe** installation file.
- On Linux: Run this command from an X Window terminal:

  ```
  bash installer-linux64.bin
  ```

  To start the installer, double-click the **installer-linux64.bin** file.

3. After you start the installer, the installation package is extracted, and the **Operations Orchestration Installation and Configuration Wizard** automatically opens. Click **Next**.



4. In the **License** page, select **I Agree**, and then click **Next**.

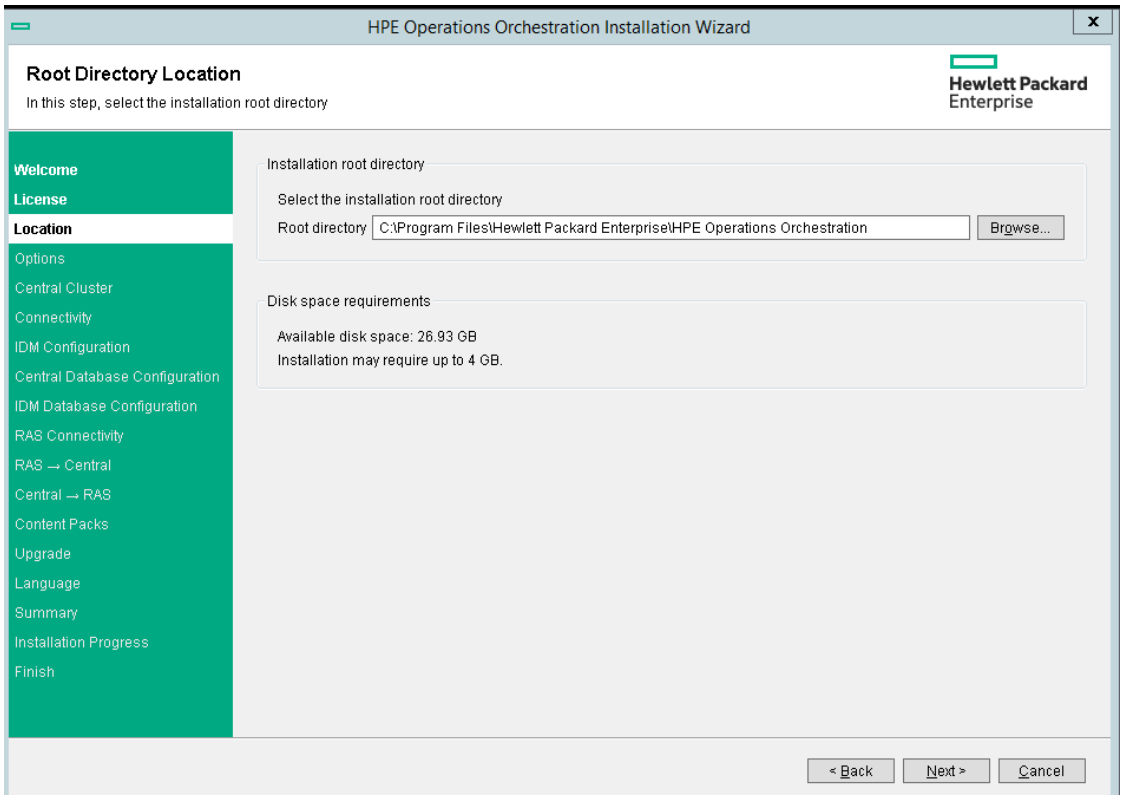
Back to the flowchart

Enter the Installation Location or Use the Default Location

1. In the **Location** page, select the location for the installation root directory.

   If the directory does not exist, the directory is created automatically. You are prompted to confirm the creation of the new location.

   > **Note:** Valid characters for the installation path are English letters, digits, spaces, hyphens (-) and underscores (_).
   >
   > The default path is `C:\Program Files\Hewlett-Packard Enterprise\HPE Operations Orchestration` for Windows and is `/opt/hpe/oo` for Linux.

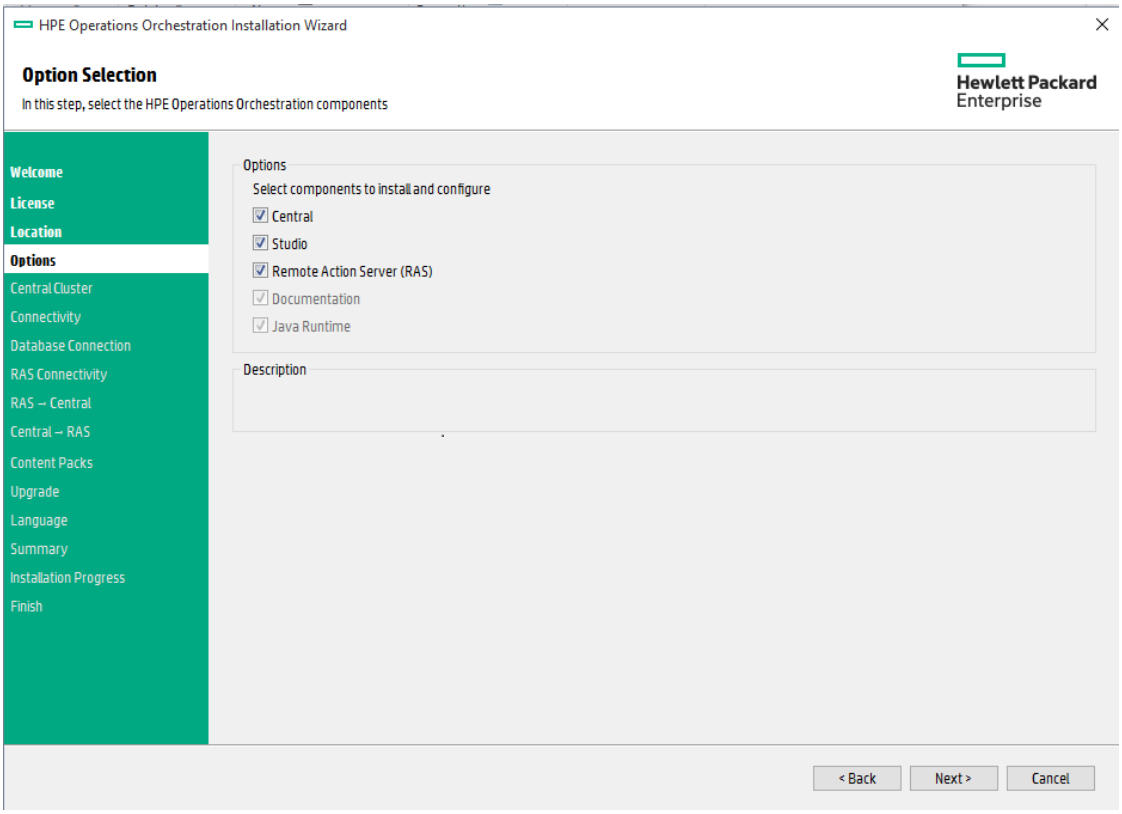


2. Click **Next**.

Back to the flowchart

Choose All the Installation Components

1. In the **Options** page, select all the check boxes.



2. Click **Next**.

Back to the flowchart

Pass Through the Cluster Step Without Modifying Anything

In the **Central Cluster** page, click **Next**.

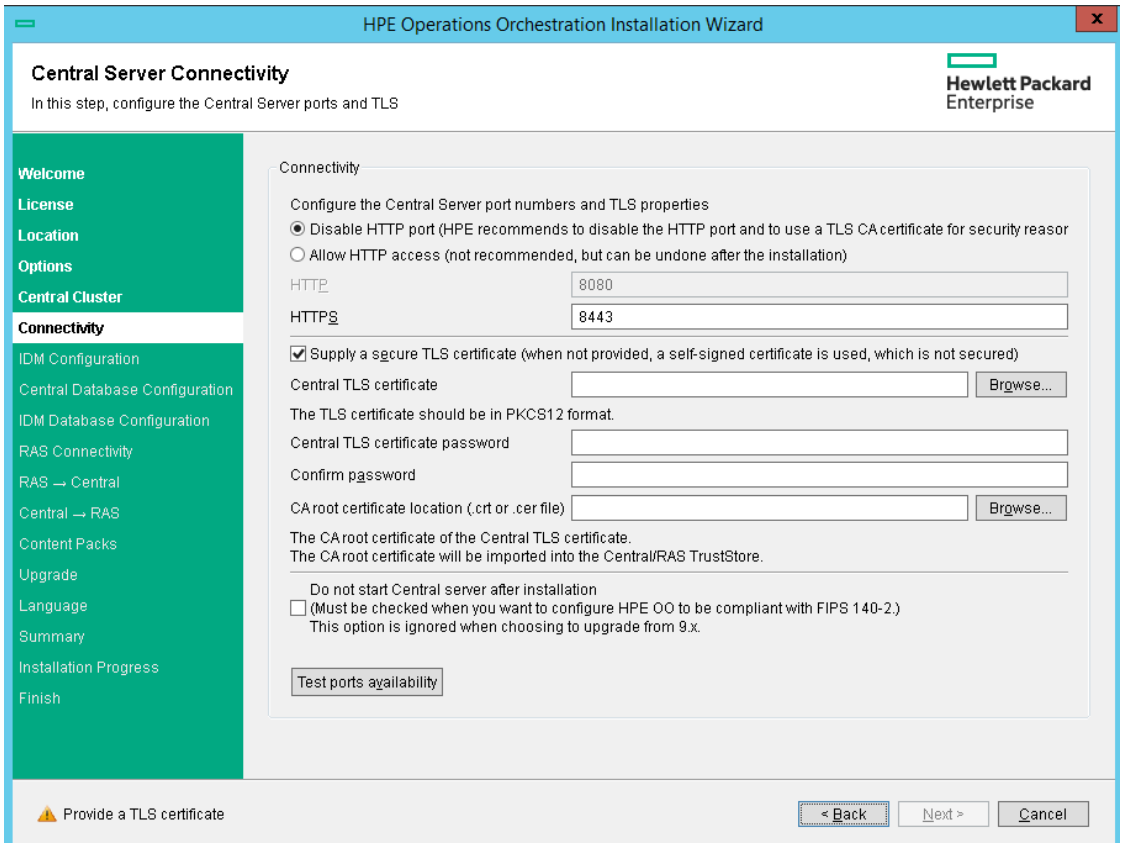
For information about how to install a node in a cluster, see "Installing an Operations Orchestration Central Cluster" on page 90.

Back to the flowchart

Decide the Port and Security Settings

In the **Connectivity** page, configure the Central Server ports and TLS:

1. Configure available ports for the Central Server. Default values (8080 and 8443) appear for each port, but you can change these. Choose one of the following options:



- (Recommended) Select **Disable HTTP Port** and configure a port in the **HTTPS** field.

  This option is recommended for security reasons, so that the communication channel is encrypted.

- (Not recommended) Select **Allow HTTP access** and configure two ports in the **HTTP** and **HTTPS** fields.

> **Note:** Configuring at least one port is mandatory. If a port is not defined, or if the ports are occupied by other applications, you will not be able to complete the installation.

2. (Recommended) Select **Provide a secure TLS certificate**, and then click **Browse** to select the certificate.

   This step is recommended, for security reasons. If you do not select a Central TLS certificate, Operations Orchestration uses a self-signed certificate.

> **Note:** Do not use a network path for the location of the Central TLS certificate.

3. If you selected a Central TLS certificate, enter its password, and enter it again for confirmation.

4. Click **Browse** to specify the location of the CA root certificate, which will be imported into the TrustStore for Central/RAS.

   > **Note:** Do not use a network path for the location of the CA root certificate.

   For more information about installing Operations Orchestration on a secured environment, see the Operations Orchestration *Security and Hardening OO Guide*.

   > **Note:** Because you are installing Central and RAS together, the **Do not start Central server after installation** option is not available. This is because the RAS server needs to connect to the Central server. If Central is not started, the installation of the RAS will fail.

Back to the flowchart

Test Ports

Click **Test ports availability**. If the ports are available, a **Success** check mark appears.

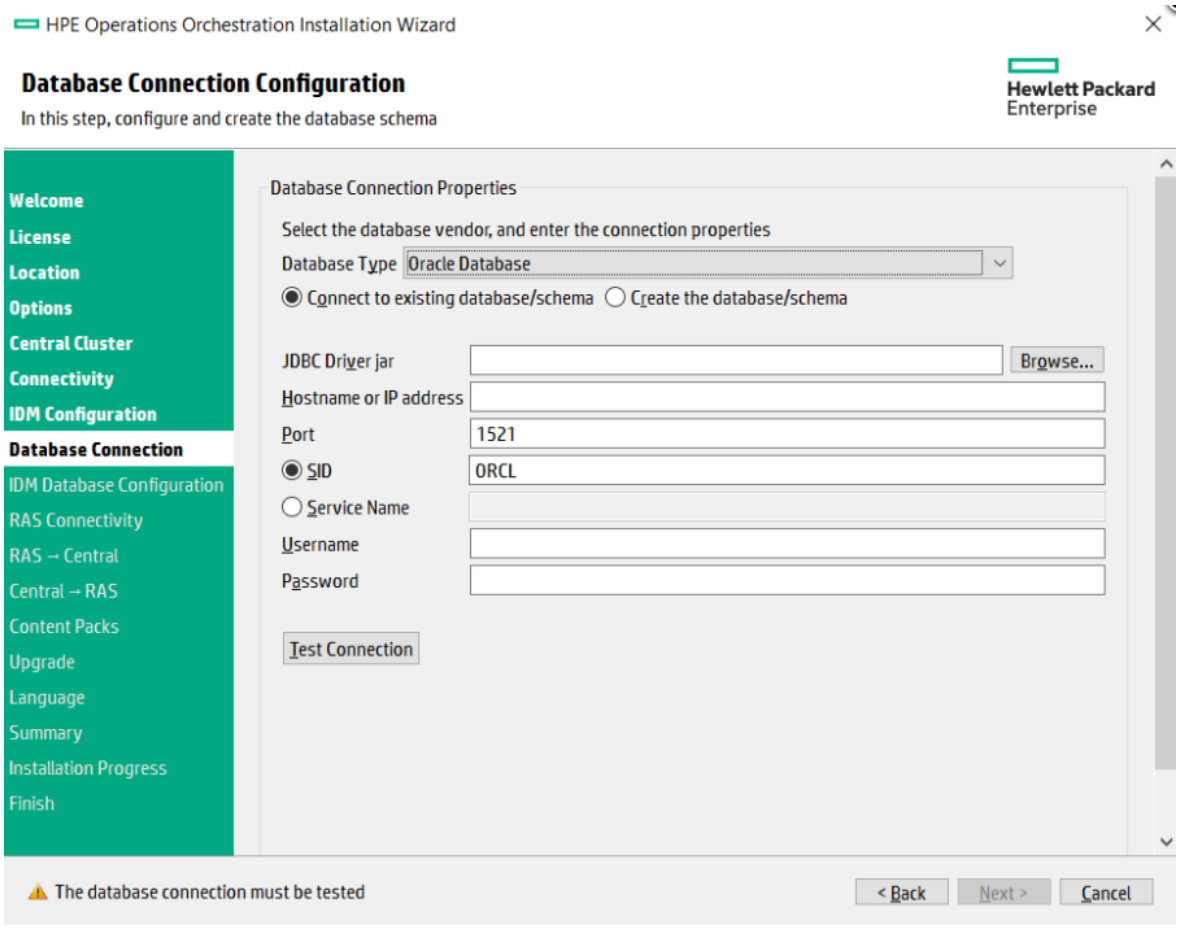
- If you encounter an error, adjust the ports accordingly and try again.
- If the **Success** check mark appears, click **Next**.

Back to the flowchart

Configure the Database

In the **Database Connection** page, you configure and create the database schema.

> **Note:** If you have user input in two languages apart from English (for example, German and Chinese) then MS SQL should not be used. You should use an alternative database such as Oracle, MySQL, or Postgres with the recommended Unicode configuration for Operations Orchestration.



1. From the **Database Type** list, select the database vendor, and then enter the connection properties.

   > **Note:** When the **Connect to existing database/schema** option is selected, do not use administrative user accounts in the **Username** and **Password** fields, because this will install Operations Orchestration under the administrative account.
   >
   > When the **Create the database/schema** option is used, provide a user with the relevant privileges in the **Admin username** and **Admin password** fields.

   You can select from the following database types:

   - **Oracle**: Do not use **SYS**, **SYSTEM**, or other administrative accounts credentials in the **Username** and **Password** fields.

     > **Note:** If you are using Oracle 11g R2 or 11g R2 RAC, it is recommended to apply patch 20299013 before installing Operations Orchestration.

   - **Microsoft SQL Server**: Do not use **sa** or other administrative account credentials in the

Username and **Password** fields.

- **Oracle MySQL**: Do not use the **root** credential in the **Username** and **Password** fields.

  If you are installing Operations Orchestration with Oracle RAC (Real Application Cluster), you must choose **Other database** and provide the URL.

- **PostgreSQL**: Do not use the **postgres** credential in the **Username** and **Password** fields.

  > **Note:** PostgreSQL database names are case-sensitive.

- **Internal database**: This uses an H2 local database. This should not be used for production.
- **Other database**: (use to enable advanced features in supported databases). If you select **Other database**, you can only use a database type that is supported for use with Operations Orchestration.

  > **Note:** The **Other database** option also supports any valid JDBC URL.

2. After selecting the database type, select one of the following:
   - **Connect to existing database/schema**: Connect to an existing schema, user, or database. The installer verifies that the schema/database and user exist.
   - **Create the database/schema**: Enables you to create a new database or schema. Information in the **Database**, **Username** and **Password** fields will be used in order to create the new schema, user, or database for Operations Orchestration.

     Confirm the password by typing it again in the **Confirm Password** field.

     Important! Make sure to use a strong password, in accordance with your organization's security policy. If the password is not strong enough, an error message will appear.

     Provide existing database user credentials in the **Admin username** and **Admin password** fields. This elevated-privileges user must be able to connect to the database and create the new schema, user, or database for Operations Orchestration.

     DBA (Admin) credentials will only be used for creating the Operations Orchestration database and user/role. It is completely safe to provide these credentials, as they not saved and not used after the Operations Orchestration installation.
3. Select the path to the Oracle JDBC driver that you installed as part of the "Pre-Installation Tasks" on page 25.
4. Enter the hostname or IP address and other connection details.

   Make sure to use the FQDN (Fully Qualified Domain Name).

If you want to use IPv6, put the IPv6 address in brackets, for example, [3fff::20]. Otherwise, errors will occur.

5. (For Oracle) Select either **SID** or **Service Name**, and enter the SID or service name of the database.

   It is recommended to use Oracle database's service name rather than using the SID.

   > **Note:** If you are upgrading from a 9.x version that is installed on Oracle, you must enter the SID of this database in the **SID** field, and not the database name.

For more information about setting up the database schema, see the *Operations Orchestration Database Guide.*

Back to the flowchart

Is the Database MySQL?

Yes: Go to Provide the JDBC Driver for MySQL

No: Go to Test Database Settings

Provide the JDBC Driver for MySQL

Complete this step if the database is MySQL:

In the **Database Connection** page, click **Browse** and select the location of the JDBC driver.

Back to the flowchart

Test the Database Settings

Click **Test Connection**. If you are unable to connect to the database, you will not be able to proceed to the next steps in the wizard.

If your password is not strong enough, a warning is displayed. You will still be able to proceed with the installation, but it is strongly recommended to replace it with a stronger password.

The installer checks for non-empty schemas/databases, and shows a warning message if the schema or database is not empty. If the installation fails during schema validation, the installation process is stopped.

> **Note:** This test only verifies the connection between Operations Orchestration and the selected database, and does not verify the conditions required by the database, like the user's read/write permissions on the provided schema.

> **Note:** For all the database vendors, if you select to create a new database, the created database

uses **case-sensitive** collation as follows:

- MySQL: **utf8_bin collation** is used for the new database.
- Postgres: Case-sensitive by design. No need for specific settings. **UTF-8** encoding is supported
- Oracle: Case-sensitive by default. No need for specific settings. **UTF-8** encoding is supported.
- MS SQL: Use only the following database collations per your required language:
  - English: SQL_Latin1_General_CP1_CS_AS
  - Japanese: Japanese_Unicode_CS_AS
  - Simplified Chinese: Chinese_Simplified_Stroke_Order_100_CS_AS
  - German: SQL_Latin1_General_CP1_CS_AS
  - French: French_100_CS_AS
  - Spanish: SQL_Latin1_General_CP1_CS_AS

However, if you already have a database installed, Operations Orchestration creates the tables using the database specific collation. It is important to note that using other collations can cause characters to appear in gibberish in the user interface for localized installations. In addition, other collations are not officially supported in Microsoft SQL Server for localized installations.

If the installer is used in order to create a new SQL Server database, selecting your language in the language selection page sets the correct collation for the new database.

Using one of the above collations enables using the **varchar** datatype for textual columns instead of the **nvarchar** data type. Using the **varchar** data type is more efficient and reduces overall database size.

Selecting a specific language also means that an Operations Orchestration system that uses SQL Server is limited to the set of languages supported by that specific collation. For example, if the **SQL_Latin1_General_CP1_CS_AS** collation is used, English, German, and Spanish characters may be used, but Japanese characters may not. If **Japanese_Unicode_CS_AS** is used, French accent characters will not be presented properly. For the complete specification of each collation, see the Microsoft SQL Server documentation.

Back to the flowchart

Select Content Packs for Studio Deployment

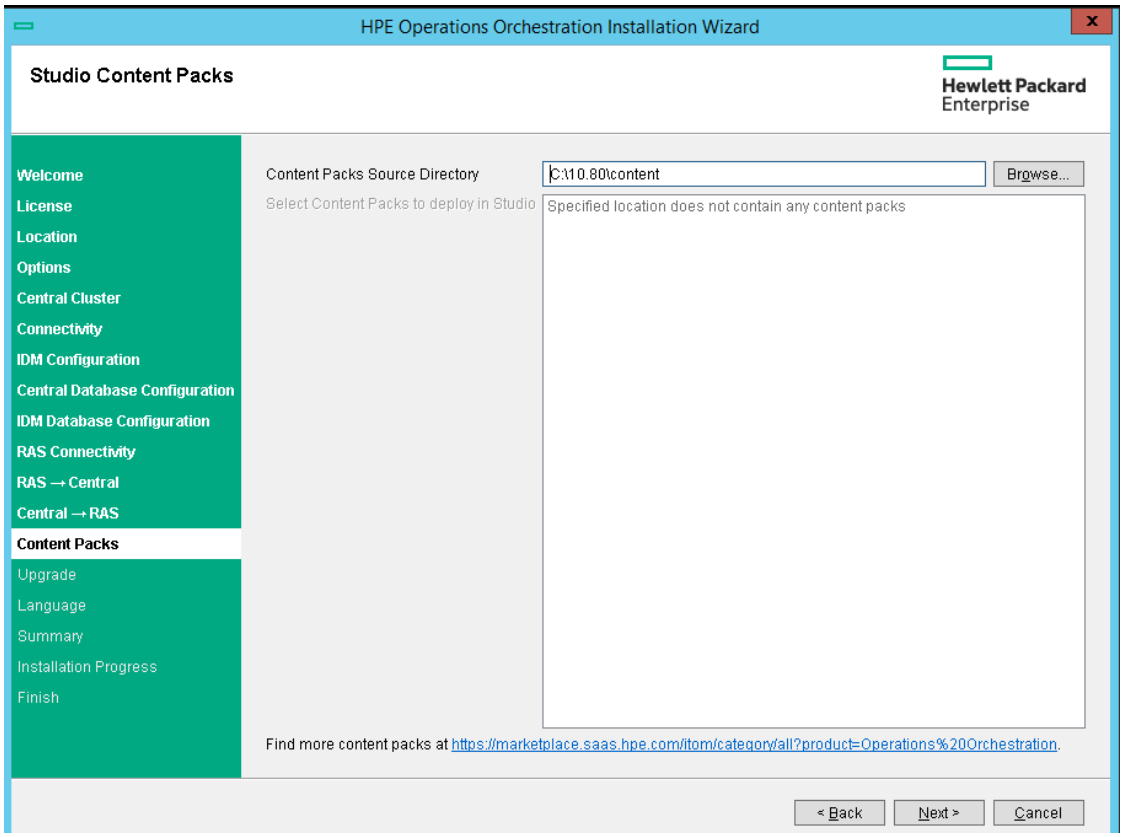
In the **Content Packs** page, you can import one or more existing content packs.

1. Browse to the location where the content packs are located, and then click **OK**.

   The available content packs located in the selected folder appear in the list.

   > **Note:** The installation folder includes the released content packs.

2. Select the content pack (or packs) that you want to import, and then click **Next**.



> **Note:** You can download additional and updated content packs on HPLN, using the link in the lower part of the wizard.

Back to the flowchart

Is it an Upgrade from 9.x?

In the **Upgrade** page, click **Next** without modifying anything.

This procedure describes how to perform a clean installation of Operations Orchestration10.x. For information about upgrading from 9.x, see the document *Upgrading to Operations Orchestration10.x from OO 9.x*.

Back to the flowchart

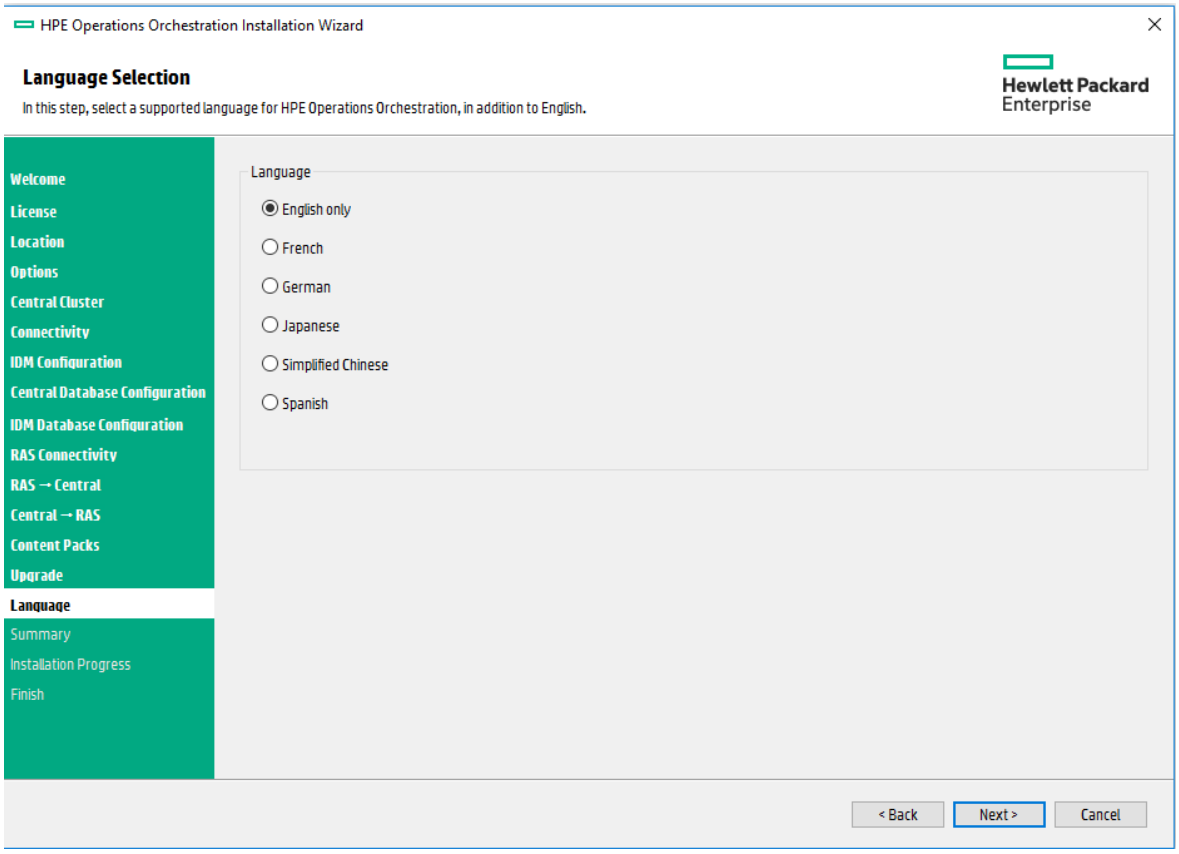
Select the Language

In the **Language** page, select a supported language for Operations Orchestration, in addition to English, and then click **Next**.

This language support will be used for:

- The MS SQL collation language, if relevant
- The **central-wrapper.conf** language for content. This language support may be required if, for example, you need to ping a server that is configured in Japanese.

> **Note:** You can change the language support choice after installation, by editing the **central-wrapper.conf** file, located in the installation directory under **central/conf**.



Back to the flowchart

Review Settings and Install

1. The **Summary** page displays the installation and configuration settings that you selected and

entered in the wizard. Check that the settings are correct. If you want to correct one of the items, click **Back**.

2. Click **Install**. The installation begins, and the wizard displays a check mark next to each successfully installed item on the **Progress** page. When the installation is complete, click **Next**.

   > **Note:** If there is a problem with one of the installation or configured items, the installation attempts to continue with the rest of the items regardless of that error. Check the **installer.log** file (the default located is **C:\HPE\oo** for Windows or in **/HPE/oo** for Linux), to check for errors.

3. (Optional) In the **Finish** page, select **Open Welcome Page** to display the Operations Orchestration Welcome page in your default web browser, in the language that was selected on the **Language** page.
4. Click **Finish** to close the Installation and Configuration wizard.

Back to the flowchart

Installation is Complete

Central, Studio, and RAS are installed and menu shortcuts are created on your system.

The installation is of the Trial version of Operations Orchestration. You will need to install the Enterprise Edition license within 90 days. For more information, see "Setting Up Licensing" in the*Operations Orchestration Central User Guide*.

After installing Studio, in order to use the Studio Git integration feature, you must install the Git client version 2.9.2. For more information, see "Installing Operations Orchestration Studio Using the Installation Wizard" on page 43.

Installing an Operations Orchestration Central Cluster

> This section is applicable only if you install Operations Orchestration 10.80 in Standalone mode. This is not applicable if you install Operations Orchestration as a container as part of suite installation.

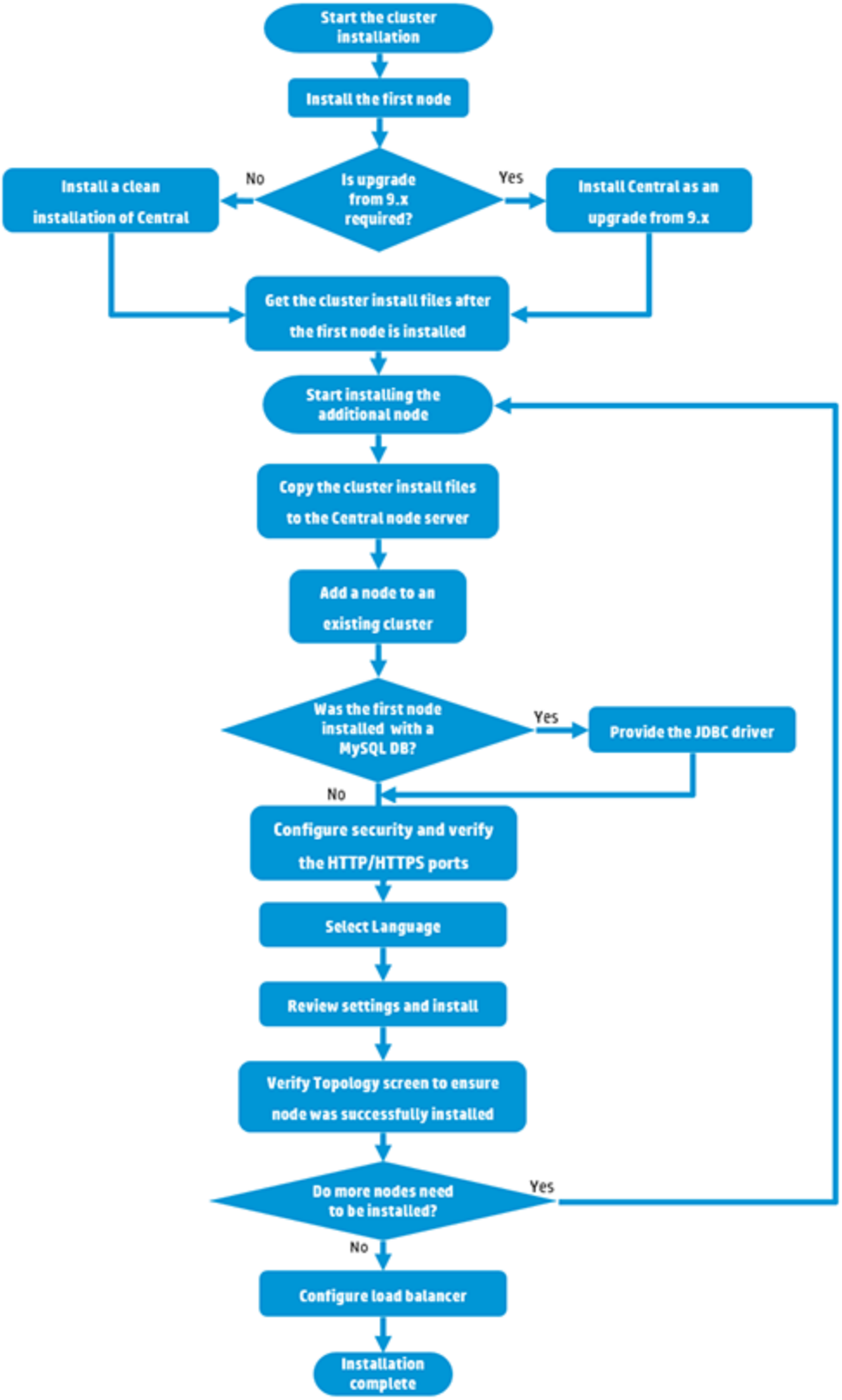
Clustering provides high availability and scalability to enhance throughput. In previous versions of Operations Orchestration, a clustering solution called Terracotta was provided as part of the application. In Operations Orchestration 10.x, this is no longer the case - there is no need for external clustering software, nor is there a requirement for a shared file system.

To create a cluster, you run the Installation wizard to create the first Central. Then, you run it again on the other machine to create the next node and, during this second installation, make it point to the same database schema.

In a clustered environment, you need to synchronize the clock times on all computers, to the second. It is recommended to use NTP sync to regularly maintain an accurate system time between all nodes (Central and RASes).

> **Note:** In a cluster environment, if a Central node is connected to a specific RAS and is shut down, the connection to the RAS is automatically moved to another working node. The RAS might be disconnected for up to three minutes. The identification may take two minutes and the RAS reconnection up to one minute.

> **Note:** This section covers how to install a cluster using a clean installation of Operations Orchestration 10.x or while upgrading from version 9.x.


Start the cluster installation
Install the first node
Is upgrade from 9.x required?
No
Yes
Install a clean installation of Central
Install Central as an upgrade from 9.x
Get the cluster install files after the first node is installed
Start installing the additional node
Copy the cluster install files to the Central node server
Add a node to an existing cluster
Was the first node installed with a MySQL DB?
Yes
Provide the JDBC driver
No
Configure security and verify the HTTP/HTTPS ports
Select Language
Review settings and install
Verify Topology screen to ensure node was successfully installed
Do more nodes need to be installed?
Yes
No
Configure load balancer
Installation complete

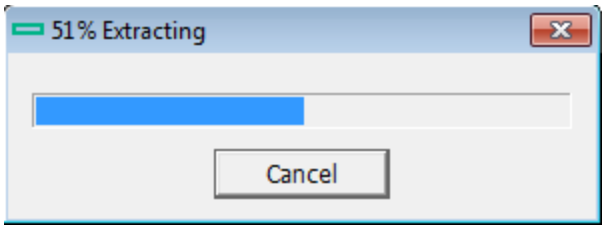
Start the 10.x Cluster Installation

Download the ZIP file from the HPE SSO Portal and extract it into a local drive on your computer.

1. To start the installer:
   - On Windows: Double-click the **installer-win64.exe** installation file.
   - On Linux: Run this command from an X Window terminal:

     ```
     bash installer-linux64.bin
     ```

     To start the installer, double-click the **installer-linux64.bin** file.
2. After you start the installer, the installation package is extracted, and the **Operations Orchestration Installation and Configuration Wizard** automatically opens. Click **Next**.



Back to the flowchart

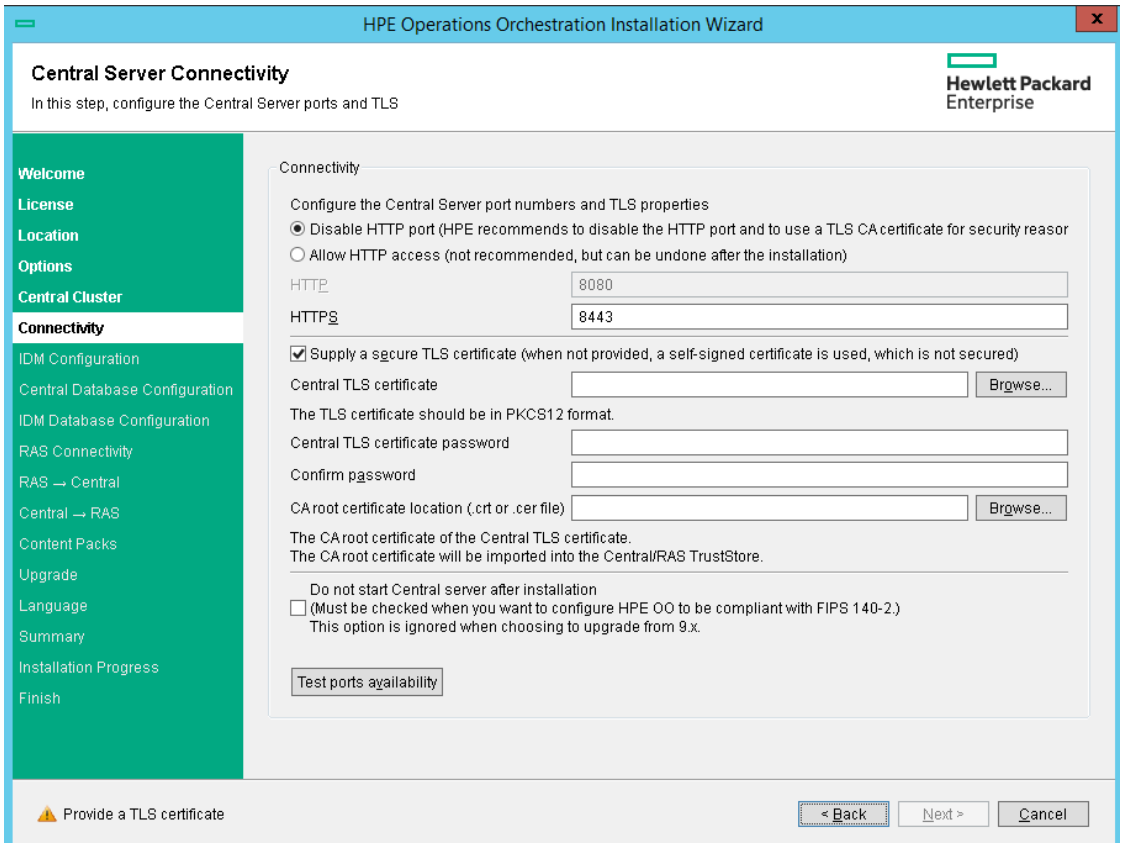
Start the Installation of the First Central Node

Install the first Central node as a stand-alone Central.

Complete the following pages in the Installation wizard. For more details, see "Installing Operations Orchestration Central with Installation Wizard" on page 28.

1. In the **License** page, select **I Agree**, and then click **Next**.
2. In the **Location** page, select the location for the installation root directory.
3. In the **Options** page, select **Central** and click **Next**.
4. In the **Central Cluster** page, click **Next**, without selecting any options.

   You will select the clustering options when you install the other nodes.
5. In the **Connectivity** page, configure available ports for the Central Server. Default values (8080 and 8443) appear for each port, but you can change these. Choose one of the following options:



- (Recommended) Select **Disable HTTP Port** and configure a port in the **HTTPS** field.

  This option is recommended for security reasons, so that the communication channel is encrypted.

- (Not recommended) Select **Allow HTTP access** and configure two ports in the **HTTP** and **HTTPS** fields.

6. (Recommended) Select **Provide a secure TLS certificate**, and then click **Browse** to select the certificate.

   This step is recommended, for security reasons. If you do not select a Central TLS certificate, Operations Orchestration uses the default self-signed certificate.

7. Enter the Central TLS certificate password, and enter it again for confirmation.
8. Click **Browse** to specify the location of the CA root certificate, which will be imported into the TrustStore for Central/RAS.

   > **Note:** Do not use a network path for the location of the certificates.

9. Select **Do not start Central server after installation** if either of the following is true:

- You are configuring Operations Orchestration to be compliant with FIPS 140-2
- You are installing a new Central in cluster mode and the installer version is older than the current Central.

> **Note:** If you are installing Central and RAS together, or upgrading from 9.x, this option is not available.

10. Click **Test ports availability**. If the ports are available, a **Success** check mark appears. If you encounter an error, adjust the ports accordingly.
11. Click **Next**.
12. In the **Database Connection** page, configure and create the database schema.

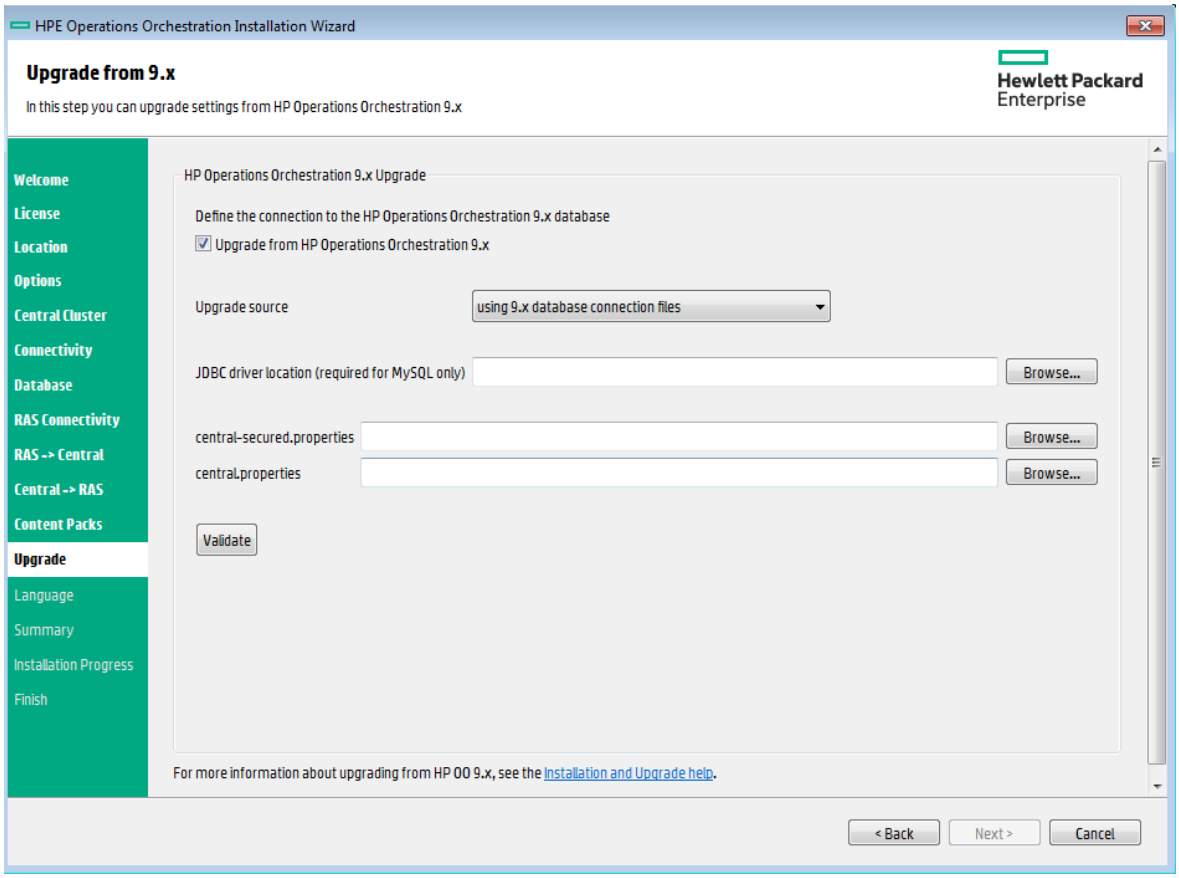
If the first node is an upgrade from 9.x, go to Yes, it is an Upgrade from version 9.x.

If the first node is a clean installation of 10.x, go to No, it is a Clean Installation of Operations Orchestration 10.x.

Back to the flowchart

Yes, it is an Upgrade from version 9.x

On the **Upgrade** page, select the **Upgrade from Operations Orchestration 9.x** check box in order to clone the database data.



Note: You only need to do this for the first Central; it is not required for other nodes.

Upgrading from 9.x to 10.x (including upgrading the 9.x content) is covered in detail in a separate document: *Upgrading to Operations Orchestration 10.x from version 9.x*. If your cluster includes an upgrade from 9.x, see *Upgrading to Operations Orchestration 10.x from version 9.x* and complete the upgrade.

When the first node has been upgraded from 9.x, continue to the next step, Get the Cluster Install Files from Central.

Back to the flowchart

No, it is a Clean Installation of Operations Orchestration 10.x

In the **Upgrade** page, click **Next** without modifying anything.

Complete the installation of the first node. For more details, see "Installing Operations Orchestration Central with Installation Wizard" on page 28.

When the first node has been installed, continue to the next step, Get the Cluster Install Files from Central.

Get the Cluster Install Files from Central

After the first Central has been installed, collect the following files.

File	Description	Location
database.properties	Defines the properties of the database.	<installation dir>/central/conf/database.properties
encryption properties	Defines how the database is encrypted.	<installation dir>/central/var/security/encryption properties
encryption_repository	Used to store the database encryption details.	<installation dir>/central/var/security/encryption_ repository
JDBC driver	This is needed only if you are using a MySQL database.	The location will vary

Start the Installation of the Cluster Node

1. Start the Installer and install the next Central node in the cluster.
2. Complete the first four pages in the Installation wizard: **Welcome**, **License**, **Location**, and **Options**.

> **Note:** If you modify the keystore password on the first node, you must apply the same configuration changes on the additional nodes.

Back to the flowchart

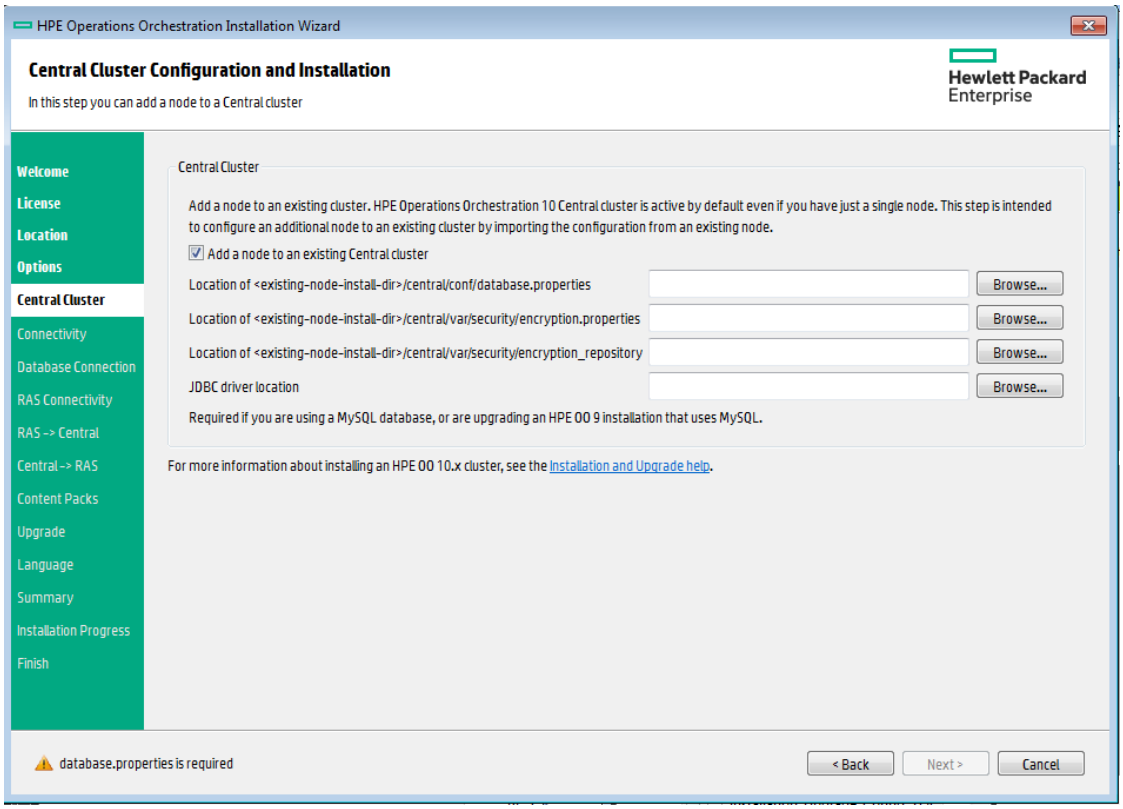
Copy the Cluster Install Nodes to the Central Node Server

Copy the cluster install files to the server on which you are installing this Central node.

Back to the flowchart

Add a Node to an Existing Cluster

1. In the **Central Cluster** page, select **Add a node to the existing Central cluster**.



> **Note:** In a cluster setting, you must not mix nodes with IDM authentication and nodes with native authentication. If the cluster to which you are adding a node uses IDM authentication, in the IDM Configuration screen select the **Connect to an existing IDM** option.

2. Click **Browse** and select the cluster files from the location where you copied them:
   - **database.properties**
   - **encryption properties**
   - **encryption_repository**

> **Note:** Once you have installed two nodes, and are installing a third, you can copy the cluster files from either server, because they contain the same data.

Back to the flowchart

Was the First Node Installed with a MySQL Database?

Yes: Go to the Provide JDBC Driver step.

No: Go to the Go to the Configure Security and Verify the HTTP/HTTPS Ports step.

Provide the JDBC Driver

If you are using a MySQL database, enter the location of the JDBC driver in the **Central Cluster** page.

Back to the flowchart

Configure Security and Verify the HTTP/HTTPS Ports

1. In the **Connectivity** page, configure available ports for the Central Server. Choose one of the following options:
   - (Recommended) Select **Disable HTTP Port** and configure a port in the **HTTPS** field.

     This option is recommended for security reasons, so that the communication channel is encrypted.
   - (Not recommended) Select **Allow HTTP access** and configure two ports in the **HTTP** and **HTTPS** fields.
2. Select **Provide a secure TLS certificate**, and then click **Browse** to select the certificate.
3. Enter the Central TLS certificate password, and enter it again for confirmation.
4. Click **Browse** to specify the location of the CA root certificate, which will be imported into the TrustStore for Central/RAS.

   > **Note:** Do not use a network path for the location of the certificates.
5. Select **Do not start Central server after installation** if either of the following is true:
   - You are configuring Operations Orchestration to be compliant with FIPS 140-2
   - You are installing a new Central in cluster mode and the installer version is older than the current Central.
6. Click **Test ports availability**. If the ports are available, a **Success** check mark appears. If you encounter an error, adjust the ports accordingly.
7. Click **Next**.

Back to the flowchart

Select the Language

In the **Language** page, you can select a supported language for Operations Orchestration, in addition to English.

Back to the flowchart

Review Settings and Install

1. The **Summary** page displays the installation and configuration settings that you selected and entered in the wizard. Check that the settings are correct. If you want to correct one of the items, click **Back**.
2. Click **Install**. The installation begins, and the wizard displays a check mark next to each successfully installed item on the **Progress** page. When the installation is complete, click **Next**.

   > **Note:** If there is a problem with one of the installation or configured items, the installation attempts to continue with the rest of the items regardless of that error. Check the **installer.log** file, located in **C:\HPE\oo** (or selected installation folder), to check for errors.

3. (Optional) In the **Finish** page, select **Open Welcome Page** to display the Operations Orchestration Welcome page in your default web browser, in the language that was selected on the **Language** page.
4. Click **Finish** to close the Installation and Configuration wizard.

Central is installed and menu shortcuts are created on your system.

Back to the flowchart

Verify Central Topology Screen to Ensure the Node was Successfully Installed

To verify that the node was successfully installed, you can check the **Topology**/**Workers** tab in Central.

1. In Central, click the **System Configuration** button.
2. Select the **Topology** /**Workers** tab and check that the node was successfully installed.
   - If a new component for Central was installed successfully (RAS or cluster node) it will appear on the screen. If there is no addition on the **Topology**/**Workers** screen after the component was installed, this means that there was a problem and you should inspect the logs.
   - The **Topology**/**Workers** screen displays the status of the worker, so you can see if the new component is viable.

     For example, the status will be red (unusable) if there are problems with certificates, failures in the operation of the worker unrelated to the initial installation, or loss of network connectivity with the component.
   - All workers display their host name and type. So the **Topology**/**Workers** screen can be used to verify any load balancer configuration issues.

For example, if there are three Centrals in the topology and only two in the load balancer, there is a clear configuration issue within the environment.

Back to the flowchart

Install Another Node

Repeat the process as often as required.

To install the next node, go back to Add a Node to an Existing Cluster.

Back to the flowchart

Configure the Load Balancer

If you are using a load balancer, reverse proxy, or DNS load balancer, configure it according to your policies. This step will vary depending on which load balancer or reverse proxy you are using. Contact your vendor for more information.

If you are using a load balancer, reverse proxy, or DNS load balancer, tell Operations Orchestration where the relevant external URL is located.

1. In Central, click the **System Configuration** button.
2. Select **Topology** > **Configuration**.
3. In the **URL** box, enter the URL of the load balancer, reverse proxy, or DNS load balancer.
4. Click **Save**.

Back to the flowchart

Installation Complete

The installation of the cluster is now complete.

After the installation of the cluster, nothing needs to be disabled. The start point and destination point of the cluster are the same. The difference between a 10.x cluster and a 9.x cluster is that you have more internal workers and you can see all Central nodes in your load balancer.

The installation is of the Trial version of Operations Orchestration You will need to install the Enterprise Edition license within 90 days.

1. Choose one of the nodes and issue a license for the IP address of this node with the HPE License Management system.
2. Open the Central UI of the specific node (and not via the Load Balancer IP) and install the license.

Installing Operations Orchestration Silently

> This section is applicable only if you install Operations Orchestration 10.80 in Standalone mode. This is not applicable if you install Operations Orchestration as a container as part of suite installation.

A silent installation is one that is started from the command line and completes without any input from the person who started it. There is no need to provide input through a wizard or dialog boxes. The silent installation receives its input from a text input file.

You can install and configure Operations Orchestration silently from a command line.

To install Operations Orchestration silently:

1. Open the **sample-silent.properties** text file (located in the **docs** folder, under the Operations Orchestration installation folder and in the **docs** folder on the ZIP file), with the required installation and configuration settings.

   For more details about these settings, see the descriptions in the **sample-silent.properties** text file.

2. Save a copy of the text file as **silent.properties**.
3. Remove the comment sign (#) from the properties that you need, and add the value for each of these properties.
4. From a command line, type the following:

   ```
   installer-win64.exe -gm2 -s c:\\temp\my-silent.properties
   ```

   To disable the extracting installation files progress bar, add to the command line `-gm2` before `-s`.

   Use the `-n` option if you don't want to start Central after the installation has completed.

   > **Note:** `gm2` is not supported with Linux.

   > **Note:** The `-s` property accepts either a full or relative path depending on the operating system:
   >
   > - Windows: Relative to the location of the `.exe` file.
   >
   >   For example: `dirA`, is the current directory, and `dirB`, is located under `dirA` and contains the installer and the **silent.properties** file. Open a Command window in `dirA` and enter the following:
   >
   >   ```
   >   dirB\\installer.exe -s silent.properties
   >   ```

> **Important**: Make sure you add two backslashes \\ and not one backslash \. The installation folder to which you download the installation file must not contain any spaces in the name.

- Linux: Relative to the location of the directory where the installer is launched.

Important Notes About Silent Installation

- Be careful not to put trailing spaces in your property values (especially when pasting). Otherwise, values that contain spaces at the end will not be read correctly and installation might fail.
- **Oracle**: Do not use `SYS`, `SYSTEM`, or other administrative account credentials in the **db.username**/**db.password** properties.
- **PostgreSQL**: Do not use **postgres** credentials in the **db.username**/**db.password** properties.

  > **Note:** PostgreSQL database names are case-sensitive.

- db.type=H2: This uses an H2 local database. This should not be used for production.
- db.type=other: Use to enable advanced features in supported databases. If you select **other**, you can only use a database type that is supported for use with Operations Orchestration. See the *Operations Orchestration System Requirements* for more information.
- Special characters, except the underscore (_), cannot be used for the database name or SID. In addition, you can enter up to 30 characters for the database name or SID.
- When you are upgrading from a remote 9.x Central that has localhost as the database in the **Central.properties** file using a silent installation, installation and upgrade do not complete successfully. This problem does not exist for wizard installations.
- All property values that contain a backslash ('\') in the **silent.properties** file need to be escaped (with a double-backslash instead of a single one).

  Places where this might be needed:

  - On Japanese environments, in all the paths given. In Japanese environments, the path separator is the Yen sign and it needs to be escaped. For example, `C:¥¥folder`
  - For RAS installations with a LDAP user given in form of 'domain\user'.
  - For a database user, if the database is set up with Windows system account authentication
  - For any other user that contains a backslash in the name

> There are some instances where the default values are different in a silent installation. For example, when installing with the wizard, by default the certificate is set to CA (user provided), while in a silent installation, this defaults to self-signed.

> **Note:** There are some instances where the default values are different in a silent installation. For example, when installing with the wizard, by default the certificate type is set to CA (user provided), while in a silent installation, this defaults to self signed. When installing with the wizard, by default the HTTP port is disabled, while in a silent installation, it defaults to enabled.

Changing the Database Settings

After installation, if you need to generate an encrypted password for the database, you can do this in the **<install_dir>/central/conf/database.properties** file.

For more information, see "Changing the Database Password" in Operations Orchestration *Administration Guide*.

Uninstalling Operations Orchestration

Before uninstalling Operations Orchestration, make sure to back up your version of Operations Orchestration.

There are two ways to uninstall Operations Orchestration:

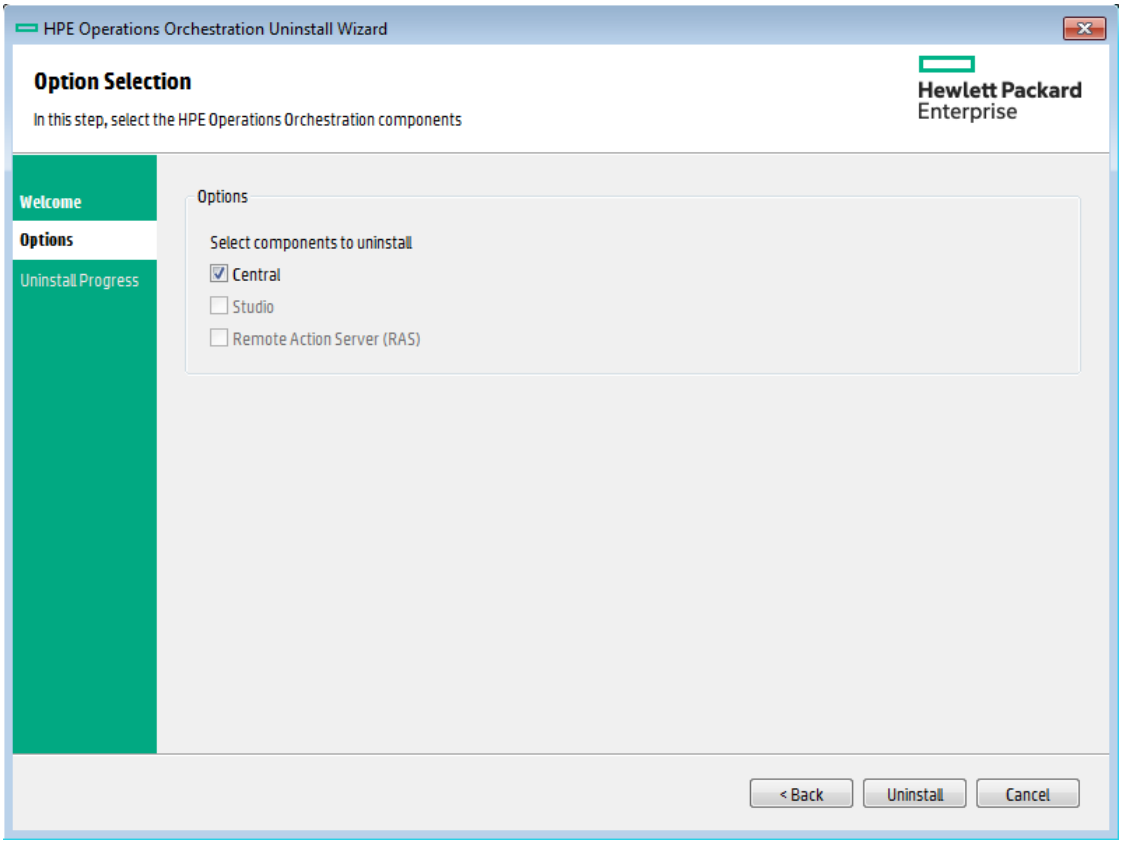
Uninstalling Operations Orchestration using the Uninstall Wizard

Uninstalling Operations Orchestration on Windows

1. In the Operations Orchestration installation directory, for example, **C:\Program Files\Hewlett Packard Enterprise\HPE Operations Orchestration**, double-click **uninstall.exe**, and then click

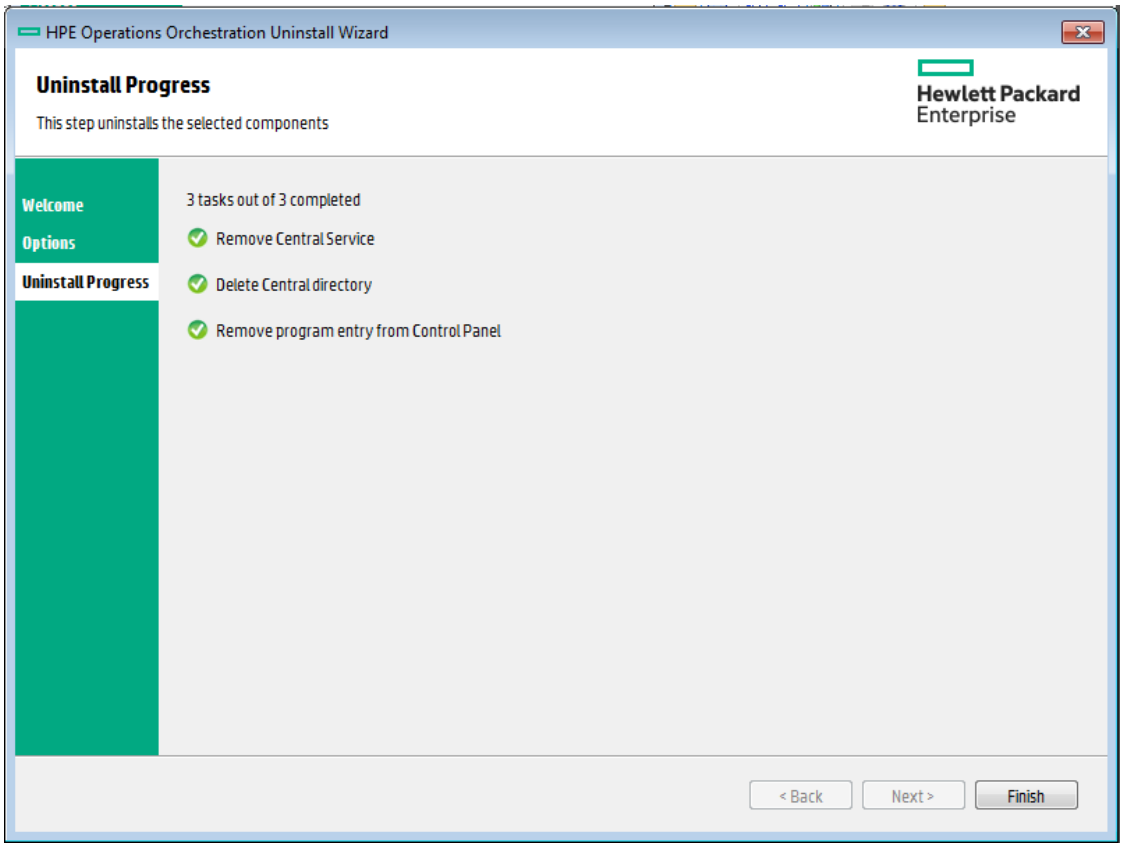
Next.

2. Select the Operations Orchestration components that you want to uninstall, and then click **Next**. When prompted whether to continue, click **Yes**.



3. The Uninstall Progress screen displays the progress of the uninstall process, and displays the items that were deleted and removed. For example:
   - Central Service
   - Central directory
   - Studio directory
   - Uninstaller control panel programs

   > **Note:** The database and database user are not removed or dropped.



4. Click **Finish**.

The selected components of Operations Orchestration are removed from your computer.

> **Note:** Uninstalling a RAS/remote worker does not remove the entry from the database. You need to also remove the RAS from Central UI, by selecting the worker in the **Topology** > **Workers** tab and using the **Delete** button. For more information, see "Setting Up Topology – Workers" in the *Operations Orchestration Central User Guide*.

Uninstalling Operations Orchestration on Linux

To uninstall Operations Orchestration in Linux, enter the following:

```
export DISPLAY=<ip address>
./uninstall
```

After the uninstall completes successfully, you can delete the installation directory.

Silent Uninstall

A silent uninstallation is one that is started from the command line and completes without any input from the person who started it. You can uninstall silently from either Windows or Linux.

To uninstall Operations Orchestration silently, type the following from a command line:

```
uninstall -s <components>
```

In the `<components>` placeholder, enter a comma-separated list of components to remove.

Possible components are: `all`, `central`, `ras`, and `studio`.

For example: `uninstall -s central,ras`

> **Note:** When you uninstall a RAS silently, if Central authentication is enabled, the RAS is not removed from the Central topology. In Central, go to **System Configuration** > **Topology** > **Workers**, and remove the RAS from the topology manually.

Hewlett Packard
Enterprise