

**opentext™**

# ALM Octane

Software version: 24.3

## Installation Guide for Windows

Go to Help Center online

<https://admhelp.microfocus.com/octane/>



Document release date: July 2024

## Send Us Feedback



Let us know how we can improve your experience with the Installation Guide for Windows.

Send your email to: [admdocteam@opentext.com](mailto:admdocteam@opentext.com)

## Legal Notices

© Copyright 2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

# Contents

Architecture .....	5
Basic configuration .....	5
Enterprise configuration .....	6
Components .....	7
Installation types .....	11
Licensing flow .....	12
Overview .....	12
Request a trial .....	12
Using Pro Edition .....	13
Install a license .....	13
Installation flow .....	14
Prerequisites .....	14
Deployment .....	15
Configuration .....	15
Start the server .....	16
Verify and log in .....	16
Configure cluster (optional) .....	16
Cluster installation flow .....	17
Prerequisites .....	21
Checklist .....	22
File system permissions .....	26
Oracle database permissions .....	26
SQL database permissions .....	28
Configure Elasticsearch .....	31
Installation .....	34
Deploy ALM Octane .....	34
Overview .....	34
Prerequisites .....	35
Deploy .....	35
Deploy in cluster environment .....	37
Configure site settings .....	37
Workflow .....	39
Database server settings .....	40

Oracle server settings .....	42
SQL Server settings .....	43
Site actions .....	44
Space settings .....	44
Elasticsearch settings .....	45
Site admin credentials .....	46
Cluster settings .....	46
Heap size .....	47
Proxy settings (optional) .....	47
Public URL and Server Ports .....	48
License settings .....	50
Authentication Type .....	50
LDAP authentication settings (optional) .....	51
SSO authentication settings (optional) .....	56
Configuration tips .....	62
Start the ALM Octane server .....	63
Log in to ALM Octane .....	64
Install ALM Octane using a Docker image .....	65
Management .....	68
Start the ALM Octane server manually .....	68
Handle database-related issues .....	69
Change site schema settings and reinitialize .....	69
Update database password in ALM Octane site schema and configuration files .....	70
Configure trust on the ALM Octane server .....	72
Using exception files for manual database changes .....	73
Overview .....	74
Define exception files .....	74
Set up use of the exception file .....	76
Advanced ALM Octane server configuration .....	78
Configure secure database access .....	78
Uninstall .....	82

# Architecture

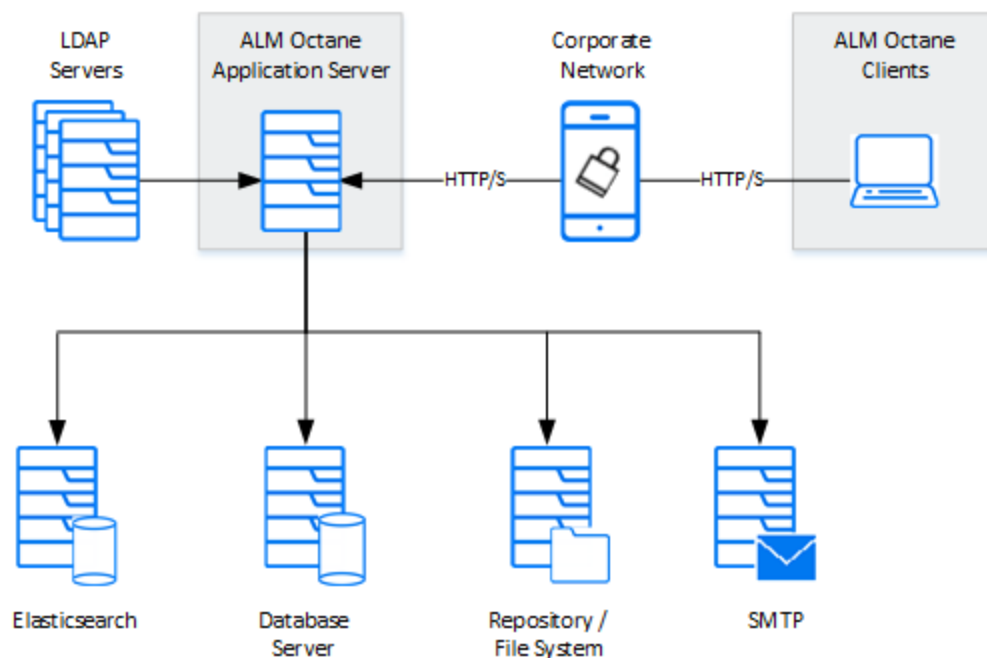
You can set up OpenText™ ALM Octane as a single node, or in a cluster configuration. The following diagrams illustrate the system architecture for both options. These are followed by descriptions of each of the components.

- ["Basic configuration" below](#)
- ["Enterprise configuration" on the next page](#)
- ["Components" on page 7](#)

## Basic configuration

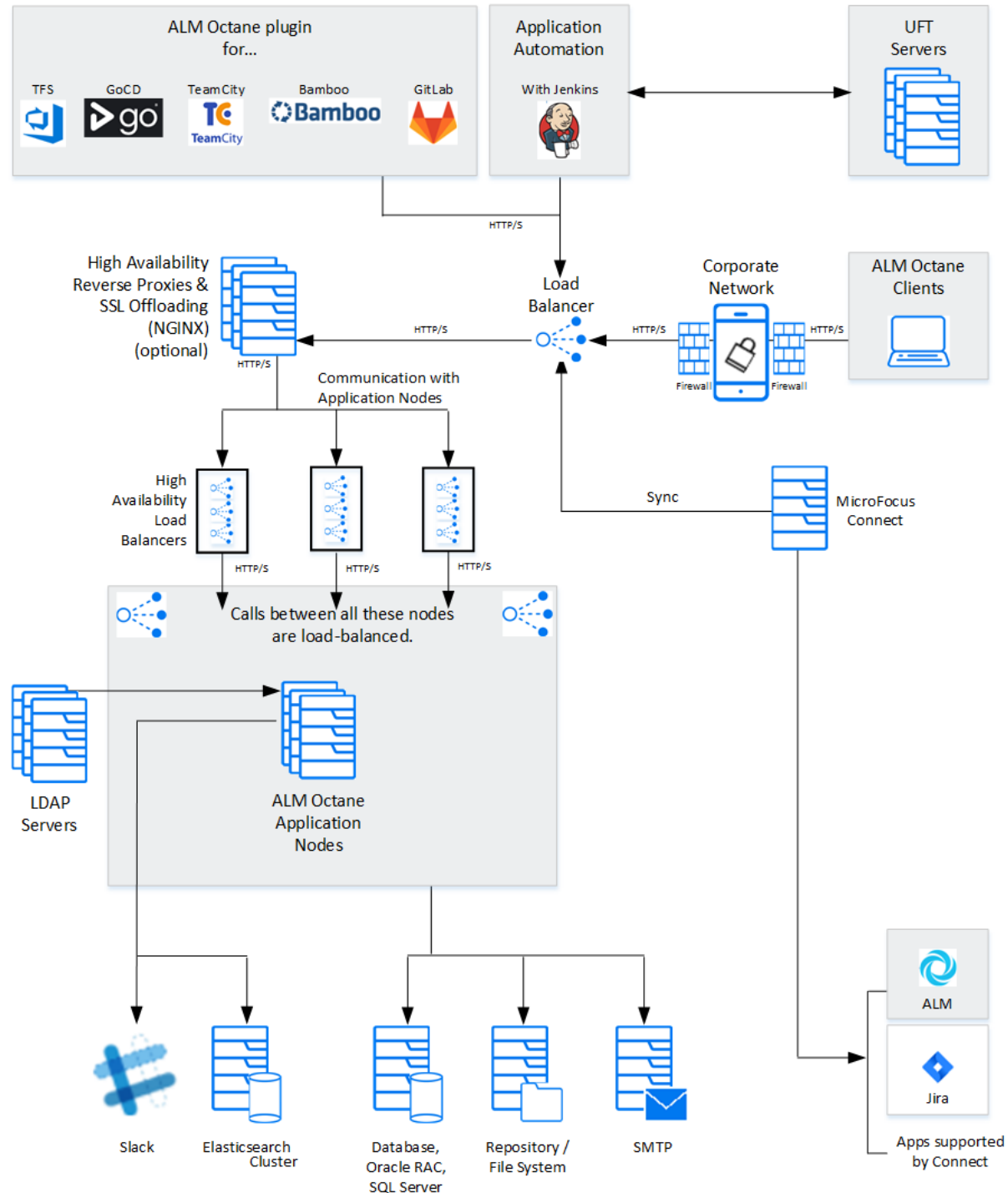
The following diagram illustrates the system architecture of a single-node configuration. Components in gray are OpenText products.

**Note:** The ALM Octane, database, and Elasticsearch servers should each reside on separate machines.



# Enterprise configuration

The following diagram illustrates the system architecture of an enterprise, cluster configuration. Components in gray are OpenText products.



# Components

Components	Description
ALM Octane clients	The clients communicate with the ALM Octane server over HTTP/S.
ALM Octane Server application nodes	Client requests from ALM Octane are dispatched to the deployed application.  <b>Note:</b> The ALM Octane, database, and Elasticsearch servers should each reside on separate machines.
ALM Octane application additional cluster (sync) nodes	<b>Cluster configuration:</b> A cluster is a group of application servers that run as a single system. Each application server in a cluster is referred to as a "node." <ul style="list-style-type: none"><li>• All nodes must have access to the database server on which the site database schema resides.</li><li>• All nodes must have access to the repository. Generally, the repository is located on an NFS or SAN server.</li><li>• All nodes must have access to each other.</li></ul>
Repository / File system	Stores all files to be used by all the projects in the system, such as templates and attachments.  <b>Cluster configuration:</b> When working in a clustered configuration, the repository must be accessible by all nodes. Also, the repository must be configured to use the same path on all nodes.

Components	Description
Database server	<p data-bbox="594 258 1409 327">A relational database management system, either Oracle RAC or Microsoft SQL Server.</p> <p data-bbox="594 352 1211 384">The database server stores the following schemas:</p> <ul data-bbox="594 409 1344 594" style="list-style-type: none"><li data-bbox="594 409 1344 510">• <b>Site schema.</b> Stores all site-related information, such as database servers, cluster nodes, the SMTP servers, and configuration.</li><li data-bbox="594 527 1344 594">• <b>Space schema.</b> All space information, such as workspaces, users, and roles.</li></ul> <p data-bbox="594 619 1409 688">This server can be shared with other applications with the following constraints:</p> <ul data-bbox="594 714 1344 930" style="list-style-type: none"><li data-bbox="594 714 1344 783">• The database must be able to sustain the load of all the applications.</li><li data-bbox="594 800 1344 930">• Future versions of ALM Octane might require a database upgrade. This may necessitate migration of data if other applications sharing the same database do not support the database version that ALM Octane requires.</li></ul> <div data-bbox="621 968 1414 1087"><p data-bbox="662 993 1398 1062"><b>Note:</b> The ALM Octane, database, and Elasticsearch servers should each reside on separate machines.</p></div>



Components	Description
Elasticsearch server (or cluster)	<p>A Java-based, open-source search engine. This component is used for various aspects of the application, such as global search and trends.</p> <p>This server can be shared with other applications with the following constraints:</p> <ul style="list-style-type: none"> <li>• The Elasticsearch engine must be able to sustain the load of all the applications.</li> <li>• Future versions of ALM Octane might require an Elasticsearch upgrade. This may necessitate migration of data if other applications sharing the same Elasticsearch do not support the Elasticsearch version that ALM Octane requires.</li> </ul> <div style="background-color: #e6f2e6; padding: 10px; border-left: 2px solid #8bc34a; border-right: 2px solid #8bc34a;"> <p><b>Note:</b> The ALM Octane, database, and Elasticsearch servers should each reside on separate machines.</p> </div> <p>A working Elasticsearch server is a requirement for working with ALM Octane. Make sure you are using a version supported by ALM Octane:</p> <p>For the supported version, see <a href="#">Database and Elasticsearch</a> in the ALM Octane Help Center.</p>
Load balancer	<p><b>Cluster configuration:</b> When working with a load balancer, client requests are transmitted to the load balancer and distributed according to server availability within the cluster.</p> <p>If you are using a load balancer, we recommend you utilize SSL offloading.</p>
High availability load balancers	<p><b>Cluster configuration:</b> These can be "VIPs" (virtual IP addresses) of one physical load balancer.</p>
DMZ	<p>An optional, demilitarized zone.</p>
High availability reverse proxies and SSL offloading	<p><b>Cluster configuration:</b> Optional configuration for load balancing using a software solution (for example, NGINX).</p>
SMTP	<p>A mail server.</p>
Jenkins (with ALM Octane plugin)	<p><b>Enterprise configuration:</b> You can integrate ALM Octane with a Jenkins CI server using the Application Automation Tools Plugin on your CI server.</p>
TFS, TeamCity, or Bamboo server (with ALM Octane plugin)	<p><b>Enterprise configuration:</b> You can integrate ALM Octane with a TFS, TeamCity, or Bamboo CI server using the Application Automation Tools Plugin on your CI server.</p>

Components	Description
Slack	Integration with Slack, which enables all stakeholders of a backlog item or pipeline run failure to collaborate and communicate. You can integrate with Slack by adding it as a collaboration tool associating it with a workspace.
Open Text testing tools: UFT Developer, UFT One, LoadRunner, LoadRunner Cloud, LoadRunner Enterprise	You can integrate ALM Octane with Open Text testing tools. For details, see <a href="#">Integrations overview</a> in the ALM Octane Help Center.

# Installation types

This document describes the necessary requirements and procedures for the installation of ALM Octane server, and initial setup steps.

Type	Description
Installation	Instructions for installing on: <ul style="list-style-type: none"><li>• A single node. For details, see <a href="#">"Installation flow" on page 14</a>.</li><li>• A cluster configuration. For details, see <a href="#">"Cluster installation flow" on page 17</a>.</li></ul>
Docker installation	A simplified installation of ALM Octane by deploying a Docker image. For details, see <a href="#">"Install ALM Octane using a Docker image" on page 65</a> .
Upgrade	For details, see <a href="#">Upgrade</a> in the Help Center.

# Licensing flow

This topic provides a high-level flow for setting up your trial license.

This section includes:

- ["Overview" below](#)
- ["Request a trial" below](#)
- ["Using Pro Edition" on the next page](#)
- ["Install a license" on the next page](#)

## Overview

To get started with ALM Octane, you begin with a 90-day on-premises free trial for 100 users. You can then install an ALM Octane license file, or allocate licenses from ALM or Quality Center.

Before you begin a trial, you should be familiar with the different editions of ALM Octane. ALM Octane is available in Enterprise and Pro Editions. For details, see [ALM Octane editions](#) in the ALM Octane Help Center.

## Request a trial

Submit a request for a free trial here: <https://www.microfocus.com/en-us/products/alm-octane/free-trial>.

When you first start using ALM Octane, you automatically receive a **Trial** license which gives you a 90-day trial for 100 users.

By default, your trial is Enterprise Edition, which allows one shared space. If you create a shared space in an Enterprise Edition trial and then install a license for Pro Edition, the trial shared space should not be used in a production environment since the sharing capabilities may not be supported in future releases.

## Using Pro Edition

There is no Pro Edition trial.

### To work with Pro Edition:

1. Install ALM Octane Enterprise Edition as your trial type, but do not create shared spaces. If you create a shared space during an Enterprise Edition trial and then install a Pro Edition license, the shared space is deactivated.
2. Get an evaluation Pro Edition license from your Sales account manager, or create a support ticket for a one-time evaluation license.
3. In the ALM Octane Settings area, apply your Pro Edition license. For details about applying licenses, see ["Install a license" below](#).

## Install a license

After you install and configure your trial instance of ALM Octane, you can purchase licenses for Enterprise or Pro Edition. You then install your license key (.dat file) in ALM Octane.

Alternatively, you can allocate your current licenses from ALM or Quality Center and share them with ALM Octane. Licenses can be allocated from ALM (ALM.Net) Edition to ALM Octane Enterprise Edition, or from Quality Center (QC) Enterprise Edition to ALM Octane Pro Edition.

**Note:** You can share up to 15% of your licenses from ALM or Quality Center, or up to 150 licenses, the lower of the two.

To learn more, see [Manage licenses](#) in the ALM Octane Help Center.

### Next steps:

- ["Installation flow" on the next page](#)

# Installation flow

This document describes the overall flow for installing the ALM Octane server on Windows.

This section includes:

- ["Prerequisites " below](#)
- ["Deployment " on the next page](#)
- ["Configuration" on the next page](#)
- ["Start the server" on page 16](#)
- ["Verify and log in " on page 16](#)
- ["Configure cluster \(optional\) " on page 16](#)

## Prerequisites

Verify your system meets hardware and software requirements.

This includes setting up permissions, opening ports, database configuration, and more.

You need three separate server machines.

- ALM Octane server
- Database server
- Elasticsearch server

For details, see ["Prerequisites" on page 21](#).

**Note:** We recommend you review security considerations in [ALM Octane Secure Deployment and Configuration Guidelines](#). This contains instructions on how to set up a secure configuration for ALM Octane.

## Deployment

Deploy ALM Octane on a machine dedicated for the ALM Octane server on Windows.

ALM Octane is deployed using an installation program.

The default deployment path is **C:\Program Files\octane**.

The command to deploy is: `octane-onprem-<version>.exe`

For details, see ["Deploy ALM Octane" on page 34](#).

## Configuration

This section describes the initial configuration.

### To configure:

1. Edit the **octane.conf** file with your site's settings for initial configuration.
2. (Optional) Depending on your needs, configure optional configuration files:
  - **elasticsearch-security.conf** to configure secure Elasticsearch.
  - **proxy.conf** to use a proxy server.
  - **ldap.conf** to use LDAP authentication.
  - **sso.conf** to use SSO authentication.

The path to these files is **<Repository folder>\conf**.

For details, see ["Configure site settings" on page 37](#).

**Note:** The .conf files do not support use of backslashes (\) in paths. Instead, use a regular slash (/) or double-slash (//).

## Start the server

Select **Start > ALM Octane > Start ALM Octane Server**.

For details, see ["Start the ALM Octane server" on page 63](#).

## Verify and log in

Verify that ALM Octane was properly installed.

Log into ALM Octane. For details, see ["Log in to ALM Octane" on page 64](#).

## Configure cluster (optional)

After starting the server on the first machine, configure and initialize each additional cluster node. For details, see ["Cluster installation flow" on the next page](#).

### Next steps:

- ["Prerequisites" on page 21](#)
- ["Deploy ALM Octane" on page 34](#)
- ["Configure site settings" on page 37](#)



# Cluster installation flow

This section provides end-to-end instructions for installing an on-premises ALM Octane server in a cluster configuration on Windows. A cluster is a group of application servers that run as a single system. Each application server in a cluster is referred to as a "node."

## To install ALM Octane in a cluster configuration:

1. For each node in the cluster, check requirements and access:

Check requirements	Verify that the all cluster nodes, including the first, meet all requirements and prerequisites. For details, see <a href="#">"Prerequisites" on page 21</a> .
Check database server access	All cluster nodes, including the first, must have access to the database server on which the site database schema resides.
Check repository access	<p>The repository directory has to be a shared directory visible to all cluster nodes. All nodes must have read and write access to the repository.</p> <p>Generally, the repository is located on an NFS or SAN server.</p> <p>The repository must be configured to use the same mount point (path) on all nodes.</p> <p>It is important that you enter the repository path using the same path name on all nodes.</p>
Check access between nodes	<p>All nodes must have access to each other. Verify ports are open in your firewall.</p> <p>ALM Octane needs to communicate between the nodes in the cluster on port 5701. Therefore, make sure that your firewall enables communication between the nodes of the cluster on the specified port..</p> <p>By default, outbound ports are open. Check inbound ports.</p>

2. Install ALM Octane on the first cluster node, as described in ["Installation" on page 34](#).
  - a. Deploy the ALM Octane installation files onto the first node. Make sure to set the **Repository folder** as a location that all cluster nodes can access.
  - b. Configure initial site settings in **octane.conf** and optional configuration files.
    - Make sure to set the **database server name** to a value that all cluster nodes can access.
    - Enter values described in ["Cluster settings" on page 46](#).

ALM Octane validates these settings when starting. If they are not valid, the ALM Octane server does not start.

- c. On the first node only, start the ALM Octane server. See ["Start the ALM Octane server" on page 63](#).
3. (Optional) If you want to set up a secure configuration for ALM Octane, follow the instructions in [ALM Octane Secure Deployment and Configuration Guidelines](#).
4. Log in to the first node in the cluster. For details, see ["Log in to ALM Octane" on page 64](#).
5. Download and deploy the ALM Octane package on each cluster node. For details, see ["Deploy ALM Octane" on page 34](#) and ["Deploy in cluster environment" on page 37](#).



**Caution:** Do not configure **octane.conf** or other configuration files. Each node is automatically configured using the configuration files located in the repository, as defined when you configured the first node.

6. On each node, start the ALM Octane server. See ["Start the ALM Octane server" on page 63](#).
7. (Optional) If you want to set up a secure configuration for ALM Octane in a cluster configuration, follow these instructions on each other node: [ALM Octane Secure Deployment and Configuration Guidelines](#).
8. Log in to make sure ALM Octane is running on each other node. For details, see ["Log in to ALM Octane" on page 64](#). Use the load balancer URL when you log in.



**Tip:** For best performance, configure your load balancer with round-robin (stateless) configuration.

9. If you need to make changes in configuration settings later, edit the **<Repository folder>\conf\octane.conf** file, and not **octane.conf.new**, which is a temporary file that is for internal use only. After modifying these settings, restart the ALM Octane server on each node to pull the configuration changes from the repository.

## Troubleshooting:

If the cluster was not properly defined, you may receive an error message when you start the ALM Octane server:

Cluster is unhealthy...

During installation, values in the hazelcast.xml file change according to the octane.conf configuration. The configuration of the hazelcast.xml file is the one that controls the cluster behavior.

Make sure that the **member** element of the hazelcast.xml file contains the same values that were defined in the **nodes** section of the octane.conf file.

## Next steps:

- ["Prerequisites" on the next page](#)
- ["Deploy ALM Octane" on page 34](#)
- ["Configure site settings" on page 37](#)

# Prerequisites

Verify that your system meets the requirements listed below, and the detailed [Support matrix](#) in the ALM Octane Help Center.


For security requirements, see the [ALM Octane Secure Deployment and Configuration Guidelines](#).


This section includes:


- ["Checklist" on the next page](#)
- ["File system permissions" on page 26](#)
- ["Oracle database permissions" on page 26](#)
- ["SQL database permissions" on page 28](#)
- ["Configure Elasticsearch" on page 31](#)

## Checklist




Use the following questions to make sure you are ready to install.

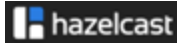
Category	Tell us...	Your answer...
	<p>On which machine will you be installing ALM Octane?</p> <hr/> <p>Does the machine have a Quad Core AMD64 processor or equivalent x86-compatible processor?</p> <hr/> <p>How much memory does the machine have? You need a minimum of 8 GB. Contact customer support for site-specific recommendations.</p> <hr/> <p>Does the machine have a minimum of 8 GB free disk space? Contact customer support for site-specific recommendations.</p> <hr/> <p>What Microsoft Windows operating system is on the machine?</p> <hr/> <p>What is the user name and password you will use for the installation user? <b>Limitation:</b> The <b>\$</b> character is not allowed in the user name or password.</p> <hr/> <p>Are your browsers and screen resolutions compatible with ALM Octane?</p> <hr/> <p>On-premises installation of ALM Octane supports only English characters for the names of schemas, operating systems, users, and so on. Did you check?</p>	

Category	Tell us...	Your answer...
	<p>Does your Elasticsearch version match ALM Octane requirements? See <a href="#">Support matrix</a> in the ALM Octane Help Center.</p>	
	<p>Do you need to download Elasticsearch?</p> <p>If you haven't installed Elasticsearch, you can download from here:</p> <p><a href="https://www.elastic.co/downloads/past-releases#elasticsearch">https://www.elastic.co/downloads/past-releases#elasticsearch</a></p>	
	<p>On which machine is Elasticsearch installed?</p>	
	<p>Did you make sure that the port for outbound communication to Elasticsearch is open?</p> <p>By default, outbound ports are open.</p>	
	<p>Did you make sure that the Elasticsearch ports (such as 9300 and 9200) are accessible directly from the ALM Octane server, not just by checking the HTTP connection?</p>	
	<p>What is the name of the Elasticsearch cluster you have configured?</p>	
	<p>Is the Elasticsearch accessible from the ALM Octane server?</p>	
	<p>Was Elasticsearch configured according to ALM Octane requirements?</p> <p>These are described in detail in "<a href="#">Configure Elasticsearch</a>" on page 31.</p>	

Category	Tell us...	Your answer...
	<p>Does your Oracle version match ALM Octane requirements? See <a href="#">Support matrix</a> in the ALM Octane Help Center.</p>	
	<p>On which machine is the database installed?</p>	
	<p>What is the Oracle database port? Default: 1521 You can modify the port in <b>octane.conf</b>.</p>	
	<p>Did you make sure that the port for outbound communication to Oracle is open? By default, outbound ports are open.</p>	
	<p>What is the URL for Java Database Connectivity (JDBC) for your database?</p>	
	<p>What is the database admin's user name and password?</p>	
	<p>Does the database admin have the necessary permissions? See "<a href="#">Oracle database permissions</a>" on page 26.</p>	
	<p>What table space and temporary table space can be used?</p>	
	<p>Did the DBA add any objects to the schemas? If so, create an exception file before installing. For details, see "<a href="#">Using exception files for manual database changes</a>" on page 73.</p>	



Category	Tell us...	Your answer...
	<p>Does your SQL Server version match ALM Octane requirements? See <a href="#">Support matrix</a> in the ALM Octane Help Center.</p>	
	<p>On which machine is the database installed?</p>	
	<p>Will you be using the SQL Server database port or instance name to connect to the database?</p> <ul style="list-style-type: none"> <li>• What is the SQL Server database port? Default: 1433</li> <li>• What is the SQL Server instance name?</li> </ul>	
	<p>What is the database admin's user name and password?</p>	
	<p>Does the database admin power user have the necessary permissions? See "<a href="#">SQL database permissions</a>" on page 28.</p>	
	<p>What MSSQL database login user, and password, can be used for ALM Octane?</p>	
	<p>Did the DBA add any objects to the databases/schemas? If so, create an exception file before installing. For details, see "<a href="#">Using exception files for manual database changes</a>" on page 73.</p>	
	<p>Do you need to install the JDK on the ALM Octane server and other servers, such as the ElasticSearch server?</p>	
	<p>Does your Java version match ALM Octane requirements? See <a href="#">Support matrix</a> in the ALM Octane Help Center.</p>	
	<p>Did you make sure that the port for inbound communication with Jetty is open?</p> <p>By default, the port is 8080. For SSL, 8443.</p> <p>You can define the port during initial installation, in <b>octane.conf</b>.</p>	

Category	Tell us...	Your answer...
	<p>Did you make sure that ALM Octane can communicate between the nodes in the cluster, using inbound and outbound communication for clusters?</p> <p>By default, the port is 5701.</p> <p>You can define the port during initial installation, in <b>hazelcast.xml</b>.</p>	

## File system permissions

The user installing ALM Octane should be an administrator on the machine, and should be able to create services.

## Oracle database permissions

Permissions depend on how you want to install ALM Octane. Do you want ALM Octane to create schemas, objects, and tables during installation, or do you want your DBA to prepare them?

Refer to the relevant section for your installation scenario:

- ["Allow ALM Octane to create Oracle schemas automatically "](#) below
- ["Create your own Oracle schemas for ALM Octane" on the next page](#)

### Allow ALM Octane to create Oracle schemas automatically

To enable ALM Octane to create schemas, tables, and objects automatically during the installation, provide ALM Octane with an Oracle power user with the following admin privileges:

- CREATE USER
- CREATE SESSION WITH ADMIN OPTION
- CREATE TABLE WITH ADMIN OPTION

- CREATE SEQUENCE WITH ADMIN OPTION
- DROP USER (optional). If not provided, the DBA must take responsibility for cleaning up unnecessary schemas.

**Note:** These permissions are for the user you will specify in the **admin-user > name** setting in the **octane.conf** file. For details, see ["admin-user > name" on page 41](#).

When defining your site action in the **octane.conf** file, you will specify **CREATE\_NEW**. For details, see ["CREATE\\_NEW" on page 44](#).

This power user can also be created temporarily, for installation purposes only. You can remove this user if:

- The installation is complete, and login to ALM Octane is successful.
- The ALM Octane site admin intends to create spaces using an existing schema, which can be selected when creating a space in the ALM Octane Settings area for the site. For details, see [Manage spaces - site admins](#) in the ALM Octane Help Center.

## Create your own Oracle schemas for ALM Octane

If you do not want ALM Octane to create schemas, tables, and objects automatically, perform the following:

1. Before installation, create two schemas with the same password.
2. Provide ALM Octane with a regular Oracle user with the following permissions, for both the site and space schemas:
  - CREATE TABLE
  - CREATE SESSION
  - CREATE SEQUENCE
  - The QUOTA clause on the user's default tablespace should be unlimited.

**Note: octane.conf**

To allow ALM Octane to use schemas you have created, you will specify the **FILL\_EXISTING** site action when defining your **octane.conf** file. For details, see "[FILL\\_EXISTING](#)" on page 44.

## SQL database permissions

Permissions depend on how you want to install ALM Octane. Do you want ALM Octane to create databases during the installation, or do you want your DBA to prepare them?

Refer to the relevant section for your installation scenario:

- "[Allow ALM Octane to create SQL databases automatically](#)" below
- "[Allow ALM Octane to create SQL databases when using Windows Authentication](#)" on the next page
- "[Create your own SQL databases for ALM Octane](#)" on the next page
- "[Create your own SQL databases when using Windows Authentication](#)" on page 30

### Allow ALM Octane to create SQL databases automatically

To enable ALM Octane to create databases automatically during the installation, use the **sa** user, or an ALM Octane database admin power user.

Install ALM Octane with a database admin power user if you cannot use the SQL **sa** user for security reasons. This user can be a temporary user, for installation purposes only.

Request that the SQL Server database admin create a temporary power user with the following privileges (roles), which are required to install ALM Octane:

- Database Creators **dbcreator** role
- Security Administrator **securityadmin** role

**Note:** These permissions are for the user you will specify in the **admin-user > name** setting in the **octane.conf** file. For details, see "[admin-user >](#)

[name" on page 41.](#)

To allow ALM Octane to create databases, you will specify the **CREATE\_NEW** site action when defining your **octane.conf** file. For details, see ["CREATE\\_NEW" on page 44.](#)

It is important that the database administrative user is not the same as the admin user. The SQL Server database admin could name this power user **octane\_install\_power\_user**, for example. For details on removing this temporary power user, see ["Handle database-related issues" on page 69.](#)

## Allow ALM Octane to create SQL databases when using Windows Authentication

1. If you are using Windows authentication, create a new Windows domain login user in your database before installing ALM Octane. Select the **Windows authentication** option, and use the credentials of a Windows domain user. Provide this user with the **sysadmin** or **dbcreator** role.
2. After installing ALM Octane, use this user to run the ALM Octane service. In the ALM Octane service properties, do not use Local system account to run the service, but rather use this user.

When defining your **octane.conf** file, you will enter **WINDOWS** as your authentication method. For details, see ["Authentication Type" on page 50.](#)

## Create your own SQL databases for ALM Octane

If you do not want ALM Octane to create databases, create two databases before installation: one for the site and one for the space.

Associate the login user to 'octane' user in both databases.

The default collation is **SQL\_Latin1\_General\_CP1\_CI\_AS** (must be case-insensitive).



**Example: Create a database and grant user access**



```
Use master
CREATE DATABASE <database_name>
GO
alter database <database_name> SET READ_COMMITTED_SNAPSHOT ON
GO
CREATE LOGIN <login_name> WITH PASSWORD = 'thepassword'
GO
USE <database_name>
CREATE SCHEMA [octane]
GO
CREATE USER [octane] FOR LOGIN WITH DEFAULT_SCHEMA= [octane]
GO
ALTER AUTHORIZATION ON Schema::octane TO [octane]
GO
ALTER ROLE [db_ddladmin] ADD MEMBER [octane]
GO
```

Run the previous commands separately for each database (site schema and space schema).



**Note:** During installation when you define the **octane.conf** file, you will enter the name of the site schema in **schemas > site**, the space schema in **schemas > initial-shared-space**, and the password in **schema-password**.

To allow ALM Octane to use databases you have created, you will specify the **FILL\_EXISTING** site action when defining your **octane.conf** file. For details, see ["FILL\\_EXISTING" on page 44](#).

## Create your own SQL databases when using Windows Authentication

1. If you are using Windows authentication, create two databases.
2. Assign the **db\_owner** role to the Windows authentication user for these databases.

You do not need to associate the login user to 'octane' user in the databases.

When defining your **octane.conf** file, you will enter **WINDOWS** as your authentication method. For details, see ["Configure site settings" on page 37](#).

# Configure Elasticsearch

Before installing ALM Octane, there are a number of settings you must configure in Elasticsearch.

**Note:** Elasticsearch supports indexes that were created in the current Elasticsearch main version, or one earlier version. Each time ALM Octane extends support for a new Elasticsearch main version, the ALM Octane upgrade includes a reindex process for the older indexes.

## Elasticsearch configuration

Before installing ALM Octane, configure Elasticsearch settings:

1. In the **elasticsearch.yml** file, configure the following:
  - **cluster.name.** Assign a unique name which will be used when you configure ALM Octane to connect to the cluster. Note that even a single-server installation is considered a cluster.
  - **node.name.** If you do not assign the node a name, Elasticsearch generates a random name on every reboot.
  - **network.host.** The node binds to this hostname or IP address and publishes this host to other nodes in the cluster. You can enter an IP address, hostname, a special value, or an array of any combination of these. Defaults to **\_local\_**.
  - **action.auto\_create\_index.** In each of your Elasticsearch cluster nodes, you must have the following line in the elasticsearch.yml files:

```
action.auto_create_index: "-mqm_*,*"
```

**Note:** If you already have an **action.auto\_create\_index** line in the yml file, add the **-mqm\_\*** phrase to the beginning of its specified value. For example, if you have the following line:

```
action.auto_create_index: "-index*,*"
```

You would change that to:

```
action.auto_create_index: "-mqm_*, -index*,*"
```

2. You can configure Elasticsearch securely using TLS. For details, see <https://softwaresupport.softwaregrp.com/doc/KM03712315>.
3. In the **jvm.options** file, set the following parameters: **-Xms<value>g** and **-Xmx<value>g**.

Define *value* as half of memory available on the machine – 1, but no more than 31GB.

## Configuring an Elasticsearch cluster

Elasticsearch can run on a single node but it is designed to run as a cluster. We do not recommend running a production environment on a single host Elasticsearch instance.

Elasticsearch clusters should have at least 3 nodes, or a larger odd number. For details see <https://www.elastic.co/guide/en/elasticsearch/reference/master/high-availability.html>.

To configure an Elasticsearch cluster, modify the following parameters in the **elasticsearch.yml**:

- **cluster.name**. This name should be identical on all nodes of the cluster to make sure they join the same cluster.
- **discovery.seed\_hosts**. To form a cluster with nodes on other hosts, use the static **discovery.seed\_hosts** setting to provide a list of other nodes in the cluster that are master-eligible, and likely to be live in order to seed the discovery process.

**Note:** The cluster nodes should be able to communicate with each other, meaning, the ports should be open in the firewall.



## Restart Elasticsearch

After changing Elasticsearch setting files (for example `elasticsearch.yml` or `jvm.options`), you must restart the Elasticsearch service.

For details on restarting an Elasticsearch cluster, see

[https://www.elastic.co/guide/en/elasticsearch/guide/master/\\_rolling\\_restarts.html](https://www.elastic.co/guide/en/elasticsearch/guide/master/_rolling_restarts.html).

## Backing up Elasticsearch

For details on backing up Elasticsearch, see

<https://www.elastic.co/guide/en/elasticsearch/reference/master/snapshot-restore.html>.

We recommend performing ELS snapshot at the same time as database backup and file repository backup.

ALM Octane does not need to be stopped for this operation.

Consider creating a batch to back up Elasticsearch data on a regular basis.

### Next steps:

- ["Deploy ALM Octane" on the next page](#)

# Installation

This section describes how to install an on-premises ALM Octane server using Microsoft Windows.

Before installing:

- Verify that your server fulfills all prerequisites. See [System Requirements](#) in the *ALM Octane Help Center*.
- Review the [ALM Octane Secure Deployment and Configuration Guidelines](#).

**Language support:** On-premises installation of ALM Octane supports only English. This means only English characters can be specified for the names of schemas, operating systems, users, and so on.

This section includes:

## Deploy ALM Octane

This section describes how to deploy the files necessary for installing an ALM Octane server.

This section includes:

- ["Overview" below](#)
- ["Prerequisites" on the next page](#)
- ["Deploy" on the next page](#)
- ["Deploy in cluster environment" on page 37](#)

## Overview

Installing ALM Octane does the following:

- Creates the correct folder structure and copies all the files to the right locations.
- Installs the ALM Octane service so that the operating system recognizes it.

## Prerequisites

Before installing:

- Verify that your server fulfills all prerequisites. See [System Requirements](#) in the *ALM Octane Help Center*.
- Review the [ALM Octane Secure Deployment and Configuration Guidelines](#).

## Deploy

This section describes how to deploy the ALM Octane package.

To deploy:

1. Download the ALM Octane package:

<https://sld.microfocus.com/mysoftware/download/downloadCenter>



**Tip:** To verify the digital signature of the RPM package, see "Installation Security" in the [ALM Octane Secure Deployment and Configuration Guidelines](#).

2. Install the ALM Octane package, by running as an administrator:

```
setup.exe
```

Click **Next**.

3. In the installation wizard panes, set the following:

<b>Installation folder</b>	The folder in which to install ALM Octane. The default is <b>C:\Program Files\octane</b> . Do not enter a name with spaces for the folder.
<b>Log folder</b>	The folder in which to create ALM Octane log files. The default is <b>C:\Program Files\octane\log</b> .

<b>Repository folder</b>	<ul style="list-style-type: none"> <li>• <b>Single node:</b> Full path of the repository folder. The default is <b>C:\Program Files\octane\repo</b>.</li> <li>• <b>Cluster installation:</b> The repository folder has to be a shared directory visible to all cluster nodes. For example, <b>MACHINE_NAME\FOLDER_NAME\repo</b>. <ul style="list-style-type: none"> <li>◦ All nodes must have read and write access to the repository.</li> <li>◦ You must enter the repository folder using the same path name on all nodes.</li> </ul> </li> </ul>
<b>Service user</b>	Whether the service should use the local system account or a specific user.
<b>Service user domain</b>	The domain of the user that will start the ALM Octane service. Available when the <b>Service user</b> is <b>Custom user</b> .
<b>Service user name</b>	The name of the user that will start the ALM Octane service. This user must have administrative permissions if using Microsoft SQL Server, and must be a local administrator. <b>Limitation:</b> The <b>\$</b> character is not allowed in the user name or password. Available when the <b>Service user</b> is <b>Custom user</b> .
<b>Password</b>	Password for the user that will start the ALM Octane service. <b>Limitation:</b> The <b>\$</b> character is not allowed in the user name or password. Available when the <b>Service user</b> is <b>Custom user</b> .
<b>Start Menu folder</b>	Location of the ALM Octane shortcuts in the <b>Start</b> menu. The default is <b>Start &gt; ALM Octane</b> .

Click **Next**. The installation starts deploying files.

4. Click **Finish**.
5. Verify that you have full administrator permissions for the following:

Default folder	Description
<b>C:\Program Files\octane</b>	ALM Octane installation folder and all its sub-directories and files. These files are used for configuring the server.
<b>C:\Program Files\octane\repo</b>	The repository folder, and its site and spaces sub-directories.

Default folder	Description
<b>C:\Program Files\octane\log</b>	Log file folder.

6. If planning to install ALM Octane on additional cluster nodes, perform the steps described under "[Deploy in cluster environment](#)" below.

## Deploy in cluster environment

This section describes how to deploy in cluster environment.

### To deploy in cluster environment:

1. **Configure the IP addresses (or fully qualified domain names) of the cluster nodes.** Configure the node IP addresses or fully qualified domain names in the **octane.conf** file. For details, see "[Configure site settings](#)" below.
2. **Verify ports are open in your firewall.** When deploying ALM Octane over a cluster, ALM Octane needs to communicate between the nodes in the cluster located on port 5701. Therefore, make sure that your firewall enables communication between the nodes of the cluster on the specified port.

## Configure site settings

Configure site settings using the ALM Octane configuration files:

- The **octane.conf** settings are mandatory for all environments.
- In addition, there are other settings that are required in complex ALM Octane environments. These include secure Elasticsearch, proxy settings, and LDAP or SSO authentication, as described below.

These settings are configured during installation, and can also be changed any time, whenever necessary.

This section includes:

- "[Workflow](#)" on page 39
- "[Database server settings](#)" on page 40

- ["Oracle server settings" on page 42](#)
- ["SQL Server settings" on page 43](#)
- ["Site actions " on page 44](#)
- ["Space settings" on page 44](#)
- ["Elasticsearch settings" on page 45](#)
- ["Site admin credentials" on page 46](#)
- ["Cluster settings" on page 46](#)
- ["Heap size" on page 47](#)
- ["Proxy settings \(optional\)" on page 47](#)
- ["Public URL and Server Ports" on page 48](#)
- ["License settings" on page 50](#)
- ["Authentication Type" on page 50](#)

## Workflow

1. Configure basic settings by editing the **octane.conf** file: `<Repository folder>\conf\octane.conf`.

In addition, depending on your environment, configure the optional files described in the following sections.

**Note:** The .conf files do not support use of backslashes (\) in paths. Instead, use a regular slash (/) or double-slash (/).

2. If you are installing ALM Octane, after editing your configuration files proceed with ["Start the ALM Octane server" on page 63](#).
3. If you need to make changes in configuration files later, make sure you edit the **<Repository folder>\conf\octane.conf** file, and not **octane.conf.new**, which is a temporary file that is for internal use only.

After modifying these settings, restart the ALM Octane server on each node to pull the configuration changes from the repository. For details, see [Modify site settings](#) in the ALM Octane Help Center.

For example, you might initially install ALM Octane to use native user management, and at a later time, decide to implement LDAP authentication for user management instead.

**Tip:** We recommend that you save a local copy of the **octane.conf** file before making changes to it. Also, for security purposes, **octane.conf** should be stored in a secure, off-site location.

## Database server settings

Setting	Description
<b>db-type</b>	Enter <b>ORACLE</b> or <b>MSSQL</b> .
<b>connection-string</b>	<p>The Java Database Connectivity (JDBC) database connection string. It includes the following details: database type, database server name, database server port number, service name.</p> <h3>Oracle connection-string</h3> <p>The instructions below demonstrate how to set up the string with non-secured database access. To configure secure access to the database, see <a href="#">"Using SSL/SSO in Oracle (optional)" on the next page</a>.</p> <p><b>Syntax using service names:</b></p> <pre>jdbc:oracle:thin:@//DB_SERVER_NAME:DB_SERVER_PORT/DB_SERVICE_NAME</pre> <p><b>Examples:</b></p> <ul style="list-style-type: none"><li>• <code>jdbc:oracle:thin:@//dbserver1.net:1521/orcl</code></li><li>• <code>jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=dbserver1.net)(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=orcl)))</code></li></ul> <div style="border: 1px solid green; background-color: #e6f2e6; padding: 5px;"><p><b>Note:</b> To connect to Oracle RAC, use the Single Client Access Name (SCAN) instead of the database server name.</p></div>
	<h3>SQL connection-string</h3> <ul style="list-style-type: none"><li>• <b>Syntax using port:</b> <pre>jdbc:sqlserver://DB_SERVER_NAME:DB_SERVER_PORT</pre><p><b>Example:</b> <code>jdbc:sqlserver://dbserver1:1433</code></p></li><li>• <b>Syntax using instance:</b> <pre>jdbc:sqlserver://DB_SERVER_NAME;instanceName=INSTANCE_NAME</pre><p><b>Example:</b> <code>jdbc:sqlserver://dbserver1;instanceName=my_instance</code></p></li></ul>



Setting	Description
<b>admin-user &gt; name</b>	ALM Octane uses the <b>admin-user</b> both to create objects during installation and also to check that the database server is accessible. <ul style="list-style-type: none"><li>• For Oracle, enter the name of the database admin user.</li><li>• For SQL Server, enter the <b>sa</b> user, or an SQL Server power user with the correct permissions.</li></ul> For details about <b>admin-user</b> permissions, see <a href="#">"Prerequisites" on page 21</a> .
<b>admin-user &gt; password</b>	The password of the database admin user. Do not include a pound sign (#) or accented characters (such as, <b>ã, ç, ñ</b> ).
<b>schemas &gt; site</b>	The name of the site schema that will be created by the <b>admin-user</b> during the installation, or supplied by the organization's DBA. Enter the supplied name.
<b>schemas &gt; initial-shared-space</b>	This parameter is relevant only for the <b>FILL_EXISTING</b> site action. If you are using <b>FILL_EXISTING</b> , set the <b>initial-shared-space</b> to the name of the schema that is designated for the space.

## Using SSL/SSO in Oracle (optional)

You can configure a secure connection from the ALM Octane server to the database server using SSL or SSO.

1. On the Oracle database server, convert the client wallet to jks keystore:

```
orapki wallet pkcs12_to_jks -wallet "<path to client wallet folder>/<client wallet folder name>" -pwd <wallet_password> -jksKeyStoreLoc <name of your jks file>.jks -jksKeyStorepwd <jks_pass>
```

For example:

```
orapki wallet pkcs12_to_jks -wallet "/home/oracle19/wallets/client_wallet" -pwd aaa123456 -jksKeyStoreLoc clientstore.jks -jksKeyStorepwd test123#456
```

2. Check the content of the newly created jks keystore:

```
keytool -list -keystore <name of your jks file>.jks -storepass <jks_pass>
```

For example:

```
keytool -list -keystore clientstore.jks -storepass test123#456
```

3. Copy the client wallet file from the Oracle database server to the ALM Octane Server. Place the newly created keystore jks file in a location on the ALM Octane app server into a directory accessible to all, such as **C:\Program Files\Octane\conf\*<name of your jks file>***.
4. Copy the following to **octane.conf**, after the **connection-string** parameter. Replace the values with the specific to your installation:

```
connection-properties : [  
    {  
        "key" : "javax.net.ssl.trustStore",  
        "value" : "<full path to keystore file>/<jks keystore  
file name>.jks"  
    }  
    ,  
    {  
        "key" : "javax.net.ssl.trustStoreType",  
        "value" : "JKS"  
    }  
    ,  
    {  
        "key" : "javax.net.ssl.trustStorePassword",  
        "value" : "<jks keystore password>"  
    }  
]
```

## Oracle server settings

Oracle settings	Description
<b>schema-password</b>	The password of the site schema. When installing using existing site schemas (with the <b>FILL_EXISTING</b> site action), make sure that the passwords that the DBA defines for the site schema and the space schema both match this <b>schema-password</b> .

Oracle settings	Description
<b>table-space</b>	The tablespace in the Oracle database where the site schema segment will be created. Case-sensitive.
<b>temp-table-space</b>	The temporary tablespace in the Oracle database. Case-sensitive.
<b>user-default-sort</b>	<p>Defines whether the standard Oracle binary sort (<b>NLS_SORT="BINARY_CI"</b>) should be overridden for non-Latin language support.</p> <p>Valid values: <b>yes</b>, <b>no</b>, or blank</p> <p><b>Default:</b> blank (yes)</p>

## SQL Server settings

SQL Server settings	Description
<b>app-user &gt; name</b>	<p>MSSQL database login authentication user for ALM Octane. This is the user for day-to-day ALM Octane use.</p> <p>This login is associated with the ALM Octane site and space databases.</p> <div style="border-left: 2px solid green; padding-left: 10px; margin-top: 10px;"> <p><b>Note:</b> This should be different from the <b>admin-user &gt; name</b>. However if you are using <b>FILL_EXISTING</b>, this must be the same as the <b>admin-user</b> name.</p> </div>
<b>app-user &gt; password</b>	<p>The password for the app-user.</p> <p>If you are using <b>FILL_EXISTING</b>, this must be the same as the <b>admin-user</b> password.</p>
<b>authentication-method</b>	Enter the authentication method used: <b>Windows</b> or <b>DB</b> (SQL Server Authentication).

## Site actions

The **SiteAction** setting determines how the installation should handle databases.

Possible values:

<b>CREATE_</b> <b>NEW</b>	<p>Use this site action for new installations.</p> <ul style="list-style-type: none"><li>• Creates a new site schema, creates a new space schema, and configures the current node.</li><li>• Only an <b>admin-user</b> with <b>create schema</b> permissions can create a new schema.</li><li>• The <b>CREATE_NEW</b> site action fails when the schema already exists.</li></ul>
<b>FILL_</b> <b>EXISTING</b>	<p>Use this site action for new installations, in cases where the database administrator does not give permissions to create a schema (for Oracle) or a database (for SQL Server).</p> <p>In this case, the organization's DBA must create a new site and space schema/database and users <b>before</b> installation.</p> <p>See the following for details:</p> <ul style="list-style-type: none"><li>• <a href="#">"Create your own Oracle schemas for ALM Octane" on page 27</a></li><li>• <a href="#">"Create your own SQL databases for ALM Octane" on page 29</a></li></ul> <p><b>Handling schema exceptions</b></p> <p>If the organization's DBA made changes to schemas, such as the addition of tables or columns, you can define an exception file. The exception file instructs ALM Octane to ignore manual changes to the database user schema during installation and upgrade. For details, see <a href="#">"Using exception files for manual database changes" on page 73</a>.</p>

## Space settings

<b>initial-space-</b> <b>mode</b>	<p>The mode in which the initial space will be created when the ALM Octane server starts. Valid values are:</p> <ul style="list-style-type: none"><li>• <b>isolated</b>. Workspaces associated with the initial space do not share entities or customization settings.</li><li>• <b>shared</b>. Workspaces associated with the initial space can share entities or customization settings.</li></ul>
--------------------------------------	--

## Elasticsearch settings

A working Elasticsearch server is a requirement for working with ALM Octane. For details on Elasticsearch prerequisites, see ["Configure Elasticsearch" on page 31](#).

<b>hosts</b>	The name of the host running Elasticsearch.  If running an Elasticsearch cluster, all node host names should be separated by commas, as follows:  <b>["host1","host2","host3"]</b>
<b>http-port</b>	Port configured in Elasticsearch for incoming HTTP requests. Default in Elasticsearch is 9200.
<b>cluster-name</b>	The name of the Elasticsearch cluster.

### Elasticsearch security (optional)

You can connect ALM Octane with Elasticsearch securely using TLS. For details, see [Setting up TLS for ALM Octane and Elasticsearch](#).

1. Make sure you have the following line in your **octane.conf** file:

```
include "elasticsearch-security.conf"
```

2. Set up the **elasticsearch-security.conf** file as follows:

<b>user</b>	<ul style="list-style-type: none"> <li>• <b>name:</b> The username to use when authenticating against Elasticsearch.</li> <li>• <b>password:</b> The password of the Elasticsearch user.</li> </ul>
<b>key-store</b>	<ul style="list-style-type: none"> <li>• <b>file:</b> The name of the PKCS12 keystore file. The file should be placed in the configuration folder.</li> <li>• <b>password</b> (optional, encrypted): The password to use to open the keystore file if the store is password protected.</li> <li>• <b>keystore type:</b> Certificate files should be in the PKCS12 format and should be put in the configuration folder.</li> </ul>
<b>trust-store</b>	<ul style="list-style-type: none"> <li>• <b>file:</b> The name of the PKCS12 truststore file. The file should be placed in the configuration folder.</li> <li>• <b>password</b> (optional, encrypted): The password to use to open the truststore file if the store is password protected.</li> <li>• <b>keystore type:</b> Certificate files should be in the PKCS12 format and should be put in the configuration folder.</li> </ul>

<b>verification-mode</b>	<p>Determine the level used when verifying the certificate. We recommend using the default setting.</p> <ul style="list-style-type: none"> <li>• <b>none</b>: No certificate verification checks are made. This means that any certificate can be accessed and should only be used to debug issues.</li> <li>• <b>certificate</b>: Only checks that the certificate is signed by a trusted CA. Should be used when hosts are dynamic.</li> <li>• <b>full</b>: In addition to certificate, also checks that the host name reported by the certificate matches the host the request is coming from. Should be used whenever possible and is the default.</li> </ul>
--------------------------	---

## Site admin credentials

<b>site-administrator &gt; name</b>	<p>The email of the site admin user that the installation creates.</p> <p>The email address can be specified now and created later.</p> <p>This is the only user available after installation. Other users can be added later.</p> <p>When using external user authentication, such as LDAP or SSO, this admin should be an existing user in the external system (LDAP or the IdP, respectively).</p>
<b>site-administrator &gt; password</b>	<p>The site admin's password. The password must be at least 8 characters long, and contain at least one uppercase letter, one lowercase letter, and one number or symbol.</p> <p>Do not include a pound sign (#) or accented characters (such as, ä, ç, ñ).</p> <p>When using external user authentication, such as LDAP or SSO, this password should be defined as a "dummy" password. It will not be used once ALM Octane is configured for external authentication.</p>

## Cluster settings

Here are some settings you must use to establish if you are installing a standalone ALM Octane server or a cluster configuration. For details on cluster configurations, see ["Cluster installation flow" on page 17](#).

<b>single-server</b>	<p>Whether your server is standalone or in a cluster configuration.</p> <p>Mandatory.</p> <ul style="list-style-type: none"> <li>• For a standalone server, set this value to <b>true</b> and do not enter any host names using the <b>nodes</b> setting.</li> <li>• For a cluster configuration, set this value to <b>false</b>. You must enter node host names in the <b>nodes</b> setting.</li> </ul>
----------------------	--

<b>nodes</b>	<p>Configure the IP addresses or fully qualified domain names for each cluster node.</p> <p>Enter a comma-separated list of node host names or IPs, in the cluster, for example:</p> <pre>["host1","host2","host3"]</pre> <p>Make sure <b>single-server</b> is set to <b>false</b>.</p>
--------------	---

## Heap size

<b>heap-size</b>	<p>Before starting the ALM Octane server the first time, change the heap memory values on all active cluster nodes.</p> <p>For example, you may need to increase the heap size if there is an increase in the number of active workspaces in ALM Octane, or an increase in the number of concurrent user sessions.</p> <p>Set <b>heap-size</b> to half of available server memory on a dedicated server, regardless of load.</p> <p>Heap size should not exceed 31 GB.</p> <p>Values should be specified in MB (for example, 4096 for 4 GB).</p> <p>Default: <b>4096</b></p>
------------------	--

## Proxy settings (optional)

If ALM Octane is behind a firewall, and needs to access an outside server, you may need to configure ALM Octane to use a proxy server.

### To configure the proxy settings:

1. Make sure you have the following line in your **octane.conf** file:

```
include "proxy.conf"
```

2. Set up the **proxy.conf** file as follows:

<b>http</b>	<ul style="list-style-type: none"> <li>• <b>host</b>: The proxy host (if using HTTP).</li> <li>• <b>port</b>: The proxy port (if using HTTP).</li> </ul>
<b>https</b>	<ul style="list-style-type: none"> <li>• <b>host</b>: The proxy host (if using HTTPS).</li> <li>• <b>port</b>: The proxy port (if using HTTPS).</li> </ul>
<b>user</b>	<ul style="list-style-type: none"> <li>• <b>name</b>: User name accessing the proxy.</li> <li>• <b>password</b>: Password for proxy user.</li> </ul>
<b>non-proxy hosts</b>	


## Public URL and Server Ports

In production systems, only secure configuration (HTTPS) is supported. In staging, we do not recommend using non-secure configuration. For details, see ["Configuration tips" on page 62](#).

Enter the following in the **server-binding** section:

<b>app-url</b>	<p>The fully-qualified domain name and port for the ALM Octane server. This is used for SSO configuration, reverse proxy configuration, SSL offloading configuration, and so on.</p> <p>This URL is also inserted as a link in emails that ALM Octane sends. Email recipients can click the link to access the relevant entity directly in ALM Octane.</p> <p>Use this pattern: <code>http://&lt;Server URL&gt;:[Port]</code></p> <p><b>Basic configuration:</b> Usually the URL of the server on which you installed the ALM Octane server.</p> <p><b>Cluster configuration:</b> The Virtual IP URL.</p> <div data-bbox="396 1010 1414 1171" style="background-color: #e6f2e6; padding: 10px;"><p><b>Note:</b> If you have a URL with a top-level domain (TLD) that is not listed in <a href="https://www.iana.org/domains/root/db">https://www.iana.org/domains/root/db</a> (for example <code>http://a.b.corp</code>, where <b>corp</b> is not listed), see <a href="#">"Configure site settings" on page 37</a>.</p></div>
<b>http-port</b>	<p>The value of a Jetty port for HTTP, or a Jetty secure port for HTTPS.</p>
<b>https-port</b>	<p>After you install ALM Octane, you may need to change the ALM Octane server port number.</p> <p>Because the installation uses a non-root user, common ports (below 1024) cannot be used with ALM Octane.</p> <p>By default, the installation uses port 8080 for HTTP or port 8443 for HTTPS (SSL).</p> <pre>httpPort: 8080 httpsPort: 8443</pre> <p>Leaving any of these ports empty disables the access using the specified http schema server.</p> <p>It is possible that the default application server port is used by another application that is running on the same machine. In this case, you can either locate the application that is using the port and stop it, or you can change the ALM Octane server port.</p>



<b>allow-http-requests-if-ssl-enabled</b>	By default, if you define your <b>app-url</b> as using HTTPS protocol, users cannot access ALM Octane via HTTP.  If you need to enable HTTP access (for example for internal tools inside your network), you can set this parameter to <b>true</b> . This allows HTTP access to ALM Octane even though your protocol is set to HTTPS.
<b>java-default-trust-store-password</b>	By default, the Java trust store password is <b>changeit</b> . If you changed this password, enter the Java trust store password here. When ALM Octane starts, it encrypts this password.  This is useful when ALM Octane server trust is configured.
<b>force-disable-http2</b>	By default, the HTTP/2 protocol is disabled, and this parameter is <b>true</b> .  To use HTTP/2, change this parameter to <b>false</b> . In this case, you must configure HTTPS using the <b>key-store</b> fields. If you are using a load balancer or proxy server, make sure that they support HTTP/2.
<b>The key-store fields are mandatory for HTTPS:</b>	
<b>file</b>	Enter the absolute path to the keystore file, or the file name if the keystore is in ALM Octane's configuration folder.
<b>password</b>	Password used to protect the keystore file. When ALM Octane starts, it encrypts this password.
<b>keystore type</b>	Enter JKS or PKCS12.   <b>Note:</b> This field must be populated (default: <b>JKS</b> ).

## Troubleshooting non-standard top-level-domains

ALM Octane validates that the top-level domain (TLD) entered in the **app-url** parameter is listed in <https://www.iana.org/domains/root/db>. If you enter a URL with a TLD that is not listed there (for example `http://a.b.corp`, where **corp** is not listed), server startup fails. In this case, perform the following steps:

1. Enter the default app-url: **https://localhost:8080**.
2. Start ALM Octane.
3. In the configuration parameters, define the parameter **ADDITIONAL\_ALLOWED\_TLD** with the value of your TLD (for example **corp**).
4. Restart ALM Octane.

- In the configuration parameters, define the parameter **SERVER\_BASE\_URL** with the correct value of your server URL (for example `http://a.b.corp`).

## License settings

<b>trial-edition</b>	The trial edition is always <b>enterprise</b> . For details, see the information about ALM Octane editions in the ALM Octane Help Center.
<b>license-mode</b>	<ul style="list-style-type: none"> <li>If you are using a standalone ALM Octane license, enter <b>standalone</b>. You can then skip the remaining fields in the <b>License</b> section. Default.</li> <li>If you are allocating licenses from ALM to ALM Octane, enter <b>ALM_SHARING</b>. You then need to fill in the following fields as described below.  For details, see <a href="#">Manage licenses (on-premises)</a> in the ALM Octane Help Center.</li> </ul>
<b>The following fields are mandatory for ALM_SHARING mode:</b>	
<b>url</b>	Enter the full path that you use to access ALM. Typically, this includes the suffix <b>qcbn</b> .
<b>integration-user &gt; name</b>	Enter the user name for accessing ALM. This user was defined in ALM for integration purposes.
<b>integration-user &gt; password</b>	Enter the password for the <b>integration-user</b> .  This password is automatically encrypted after you restart the ALM Octane server.

## Authentication Type

Specify whether the ALM Octane installation should use native user management (default), LDAP, or SSO authentication for user management.

<b>authentication-type</b>	<p>Values are:</p> <p><b>internal</b>. Use internal, native ALM Octane user management. Default.</p> <p><b>ldap</b>. Use LDAP authentication. Define LDAP settings as described in "<a href="#">LDAP authentication settings (optional)</a>" on the next page.</p> <p><b>sso</b>. Use SSO authentication. Define SSO settings as described in "<a href="#">SSO authentication settings (optional)</a>" on page 56.</p>
----------------------------	--

## LDAP authentication settings (optional)

If you plan on authenticating users using LDAP, we recommend you configure LDAP settings using the ALM Octane Settings UI after installation, rather than in the **ldap.conf** file. When you configure LDAP in the Settings UI, your settings are automatically validated and updated in the **ldap.conf** file. For details, see [Configure LDAP](#) in the ALM Octane Help Center.

If you prefer to work directly in the configuration files rather than in the Settings UI:

1. Make sure you have the following line in your **octane.conf** file:  

```
include "ldap.conf"
```
2. In the **ldap.conf** file, configure the LDAP settings as described below.
3. Later, after ALM Octane installation, import users from LDAP into ALM Octane.

**Tip:** LDAP settings are validated when you start ALM Octane. If there are errors in your LDAP configuration which prevent the ALM Octane server from starting, have a site admin check the wrapper, site, and app logs.

### General LDAP settings

Field	Description
<b>connection-timeout</b>	Connection timeout in seconds. Optional. Default: 30 seconds

Field	Description
<b>admin-dn</b>	<p>The user that signs in to ALM Octane after <b>initially</b> setting up LDAP authentication. Its purpose is to make sure that one workable user exists to start configuring LDAP user authentication.</p> <p>When the ALM Octane server starts, it checks LDAP configuration settings, verifies that this user exists, and validates this user against the LDAP data. If this attribute is not defined correctly, the server does not start. Correct the user details and restart the server.</p> <p>This user can be same user as the user entered in the <b>octane.conf</b> file, or a different user. After entering the value for this user, and then restarting the ALM Octane server, the admin user entered in the <b>octane.conf</b> file is overwritten. This becomes the ALM Octane site admin user that can be used to log into ALM Octane the first time.</p> <p><b>Note:</b> If the <b>admin-dn</b> is changed and the server is restarted, both the original <b>admin-dn</b> and the new <b>admin-dn</b> exist as site admins. Modifying the <b>admin-dn</b> does not remove the original one.</p>

## LDAP server settings

Enter the following settings for each LDAP server separately.



**Caution:** Back up all passwords set below because they are encrypted after the ALM Octane server is initialized.

<b>servers</b>	Header row to delineate that the information below is for each LDAP server. Do not enter a value.
<b>host</b>	The LDAP server host name or IP address. Mandatory.
<b>port</b>	LDAP server connection port. Mandatory.
<b>ssl</b>	<p>Whether the LDAP server uses SSL. Mandatory.</p> <p>Enter <b>Y</b> or <b>N</b>.</p> <p>If <b>Y</b>, establish trust to the certificate authority that issued the LDAP server certificate. For details, see "<a href="#">Configure trust on the ALM Octane server</a>" on <a href="#">page 72</a>.</p>

<b>base-directories</b>	<p>Root of the LDAP path to use to search for users when including new LDAP users in ALM Octane spaces. This can be a list of common names and domain components (cns and dns), a list of organizational units (ou), and so on.</p> <p>Optional. Default: Blank.</p> <p><b>Example:</b></p> <pre>"base-directories" : [     "dc=maxcrc,dc=com",     "ou=Administrative,dc=maxcrc,dc=com" ],</pre>
<b>base-filters</b>	<p>Filters to use to refine the search for users when including new LDAP users in ALM Octane spaces. This is generally a semi-colon delimited list of LDAP <b>objectClasses</b>.</p> <p>Optional. Default: (objectClass=*)</p>
<b>description</b>	Description of the LDAP server. Optional.
<b>authentication:</b>	Header row to delineate that the information below is for authentication. Do not enter a value.
<b>method</b>	<p>The LDAP authentication method supported by the LDAP server. Authentication method used by the LDAP server. The following methods are supported:</p> <ul style="list-style-type: none"> <li>• <b>anonymous</b>. In this case, skip the next two parameters, <b>name</b> and <b>password</b>.</li> <li>• <b>simple</b>. <b>name</b> and <b>password</b> are mandatory.</li> </ul>
<b>user name</b>	<p>Only required if you set the <b>authentication</b> parameter to <b>simple</b>.</p> <p>User name for accessing the LDAP server. This user must have at least read permissions for the LDAP server.</p>
<b>password</b>	<p>Only required if you set the <b>authentication</b> parameter to <b>simple</b>.</p> <p>Password for accessing the LDAP server.</p> <p>This password will be encrypted.</p>

## LDAP server mapping settings

Enter the following mapping settings for each LDAP server separately.

Values used in the mapping section are case-sensitive.

ALM Octane attribute in ldap.conf	Sample LDAP attribute that can be used	Values and descriptions
<b>mapping</b>		Header row to delineate that the information below is for mapping of LDAP attributes. Do not enter a value.
<b>dn</b>	<b>distinguishedName</b>  <b>(for Active Directory)</b>	<p>The LDAP distinguished name attribute. Unique. Mandatory.</p> <p>This attribute is typically in a format that contains the common name and organization details, such as:</p> <p><b>cn=&lt;common_name&gt;,ou=&lt;organizational_unit&gt;,dc=&lt;part_of_domain&gt;</b></p> <p>The <b>dn</b> is a unique string that typically contains other LDAP attributes, such as <b>cn</b>, <b>ou</b>, and <b>dc</b>.</p>
	<b>entryDN</b>  <b>(for other LDAP systems)</b>	<p><b>Example</b></p> <ol style="list-style-type: none"> <li>1. If in LDAP, the <b>entryDN</b> attribute value is: <b>cn=&lt;common_name&gt;,ou=&lt;organizational_unit&gt;,dc=&lt;part_of_domain&gt;</b></li> <li>2. In the <b>ldap.conf</b>, the dn value would be mapped to: <b>entryDN</b></li> <li>3. When exporting users from LDAP, the <b>dn</b> string representation of each LDAP user would be the common name, followed by the organizational unit, followed by a part of the domain, such as: <b>cn=Joe_Smith@nga,ou=my_org,dc=com</b></li> </ol>

ALM Octane attribute in ldap.conf	Sample LDAP attribute that can be used	Values and descriptions
<b>uid</b>	<p><b>objectGUID</b> <b>(for Active Directory)</b></p> <hr/> <p><b>entryUUID</b> <b>(for other LDAP systems)</b></p>	<p>The LDAP attribute that should be used as the immutable, globally-unique identifier. Mandatory.</p> <p>In this documentation, we also refer to this as the UUID (universally unique ID).</p> <ul style="list-style-type: none"> <li>• For Active Directory: To work with ALM Octane with Active Directory, we use <b>objectGUID</b>.</li> <li>• For other LDAP systems: To work with ALM Octane, we generally use <b>entryUUID</b> for OpenLDAP. However, depending on your LDAP, this attribute might be different, such as <b>GUID</b> or <b>orclguid</b>.</li> </ul> <p>This is an attribute by which ALM Octane identifies each user internally for synchronization between ALM Octane and LDAP, including when importing users into ALM Octane.</p> <p>You can configure other values, such as GUID or orclguid, or any other unique value.</p>
<b>first-name</b>	<b>givenName</b>	LDAP attribute for first name, such as <b>givenName</b> . Mandatory.
<b>last-name</b>	<b>sn</b>	LDAP attribute for last name, such as <b>sn</b> . Mandatory.
<b>full-name</b>	<b>cn</b>	LDAP attribute for full name, such as <b>cn</b> . Optional.
<b>logon-name</b>	<b>mail</b>	<p>This is the unique identifier between all ALM Octane users, and this attribute is used to log onto ALM Octane.</p> <p>In some cases, ALM Octane may use this attribute to identify each user internally for synchronization between ALM Octane and LDAP, including when importing users into ALM Octane.</p> <p><b>mail</b> is usually unique for each user, so <b>mail</b> is an appropriate LDAP attribute to use to map to <b>logon-name</b>. Mandatory.</p> <p>You can change the <b>logon-name</b> attribute mapping at any time, but make sure the <b>logon-name</b> is unique across all ALM Octane users.</p>
<b>email</b>	<b>mail</b>	The LDAP attribute for email address, such as <b>mail</b> . Mandatory.
<b>phone1</b>	<b>telephoneNumber</b>	The LDAP attribute for the primary phone number, such as <b>telephoneNumber</b> . Optional.

## SSO authentication settings (optional)

Use these settings to set up SSO authentication for connecting to ALM Octane with an external IDP.

### To configure the SSO authentication settings:

1. Make sure you have the following line in your **octane.conf** file:

```
include "sso.conf"
```

2. Set up the **sso.conf** file as follows:

#### Key-pair settings:

Setting	Description and usage
<b>alias</b>	Unique identifier for the SSO public/private key pair used by the ALM Octane service provider for signing and encrypting authentication information.  Mandatory.  Example: <b>sso-osp-keypair</b>
<b>password</b>	Password for protecting and encrypting the key pair defined with <b>key-pair alias</b> .  When ALM Octane starts, it encrypts this password.  Mandatory.  Example: <b>my-secret</b>

#### Key-store settings:

Setting	Description and usage
<b>file</b>	The absolute path to the keystore file identified with <b>key-pair alias</b> .  The path should be under ALM Octane's configuration folder to avoid permission issues.  Mandatory.



Setting	Description and usage
<b>password</b>	<p>Password used to protect the keystore file defined with <b>keystore file</b>.</p> <p>When ALM Octane starts, it encrypts this password.</p> <p>Mandatory.</p> <p>Example: <b>my-password</b></p> <div style="background-color: #e6f2e6; padding: 5px;"><p><b>Note:</b> If you are using pkcs12, you must use the same password for both the keystore and the key(s). This is a Java limitation.</p></div>
<b>keystore-type</b>	<p>This defines the keystore type. The default format for this file is <b>PKCS12</b>. You can change the format to Java KeyStore (JKS) by specifying this type here.</p>

### OAuth settings:

Setting	Description and usage
<b>client-id</b>	<p>Client ID used for internal OAuth2 configuration and by which the integration that will be accessing ALM Octane will identify itself.</p> <p>Regular expressions are not supported (meaning, no asterisk wildcards).</p> <p>Must be the same on all ALM Octane cluster nodes.</p> <p>Mandatory.</p> <p>Example: <b>my-client-ID</b></p>
<b>client-secret</b>	<p>The OAuth client secret for the integration's client ID defined with <b>oauth client-id</b>.</p> <p>Can be any value. We recommend that the secret be complex and hard to guess.</p> <p>Must be the same on all ALM Octane cluster nodes.</p> <p>When ALM Octane starts, it encrypts this password.</p> <p>Mandatory.</p> <p>Example: <b>secret</b></p>

Setting	Description and usage
<b>authentication-timeout</b>	<p>The SSO authentication timeout in seconds.</p> <p>Optional.</p> <p>Default: <b>10800</b> seconds (3 hours).</p> <p><b>Other timeout settings when working with SSO</b></p> <p>The following configuration parameters can be used to set other timeouts when working with SSO. These parameters are defined in the Settings area in ALM Octane, not in the <b>sso.conf</b> file. They do not have any effect on the SSO authentication timeout.</p> <ul style="list-style-type: none"> <li>• <b>MINUTES_UNTIL_IDLE_SESSION_TIMEOUT</b>. Defines license consumption in minutes.</li> <li>• <b>MINUTES_UNTIL_GLOBAL_SESSION_TIMEOUT</b>. Defines API key authorization timeout in minutes.</li> </ul> <p>For details on setting these configuration parameters, see <a href="#">Configuration parameters</a> in the ALM Octane Help Center.</p>

### SAML settings:

Section	Setting	Description and usage
<b>IdP</b>	<b>metadata-url</b>	<p>The IdP's URI for publishing IdP metadata. Part of the pairing process. If this is set, there is no need to set metadata. Using this option, the URL must be available and respond with a valid XML or ALM Octane will not start.</p> <p>Any valid URL is accepted.</p> <p>You can define the SAML metadata descriptor resource with either this setting, or the <b>saml idp metadata</b> setting.</p> <p>Mandatory, if <b>saml idp metadata</b> is not defined.</p> <p>Example: <b>http://my-server.company-infra.net:8080/auth/realms/Dev/protocol/saml/descriptor</b></p> <p><b>Note:</b> Only one of the parameters <b>metadata</b> or <b>metadata-url</b> should be defined. If the sso_configuration validator is disabled and both parameters are defined, the URL defined in <b>saml idp metadata-url</b> will be ignored.</p>

Section	Setting	Description and usage
<b>IdP</b>	<b>metadata</b>	<p>Base 64 encoded XML of the SAML metadata descriptor from the IdP. This should be used if the IdP metadata URL cannot be accessed from the ALM Octane server.</p> <p>You can define the SAML metadata descriptor resource with either this setting, or the <b>saml idp metadata-url</b> setting.</p> <p>Mandatory, if <b>saml idp metadata-url</b> is not defined.</p> <p><b>Note:</b> Only one of the parameters <b>metadata</b> or <b>metadata-url</b> should be defined. If the sso_configuration validator is disabled and both parameters are defined, the URL defined in <b>saml idp metadata-url</b> will be ignored.</p>
<b>Mapping</b>	<b>user-name</b>	<p>The parameter in the SAML response which maps to the user name.</p> <p>Valid values are:</p> <ul style="list-style-type: none"> <li>• <b>{\$id}</b>. Mapping is to the <b>NameID</b> in the SAML response's subject. Default.</li> <li>• <b>userName</b>. Mapping is to the <b>username</b> in the SAML attribute statement.</li> </ul> <p>Changing the default to a property name, such as <b>userName</b>, in the SAML response, does not require quotes.</p>
<b>Mapping</b>	<b>uuid</b>	<p>The attribute in the SAML response's attribute statement that maps to the user's UUID.</p> <p>Optional.</p> <p>Default: <b>uuid</b></p>
<b>Mapping</b>	<b>mail</b>	<p>The attribute in the SAML response's attribute statement that maps to the user's email address.</p> <p>Optional.</p> <p>Default: <b>mail</b></p>
<b>Mapping</b>	<b>first-name</b>	<p>The attribute in the SAML response's attribute statement that maps to the user's first name.</p> <p>Optional.</p> <p>Default: <b>firstName</b></p>
<b>Mapping</b>	<b>last-name</b>	<p>The attribute in the SAML response's attribute statement that maps to the user's last name.</p> <p>Optional.</p> <p>Default: <b>lastName</b></p>

Section	Setting	Description and usage
<b>Mapping</b>	<b>full-name</b>	The attribute in the SAML response's attribute statement that maps to the user's full name.  Optional.  Default: <b>fullName</b>

### Token-exchange settings:

Setting	Description and usage
<b>token-exchange-enabled</b>	Activates the federated identity option for authenticating APIs within an organization's SSO system.  Mandatory.  Default: <b>false</b>
<b>issuer</b>	Used to define the <baseUrl> in any OpenID Connect (OIDC) endpoint when authorizing against the external OAuth 2.0 authorization server. Use the following endpoints to review the metadata and find the issuer:  <b>https://&lt;OAuth2 Authorization Server&gt;/.wellknown/openid-configuration</b>  Mandatory.
<b>treat-access-token-as-opaque</b>	If <b>true</b> , any access token returned from the OIDC provider is treated as an opaque token even if it appears to be a JWT token. Set to <b>true</b> only if the provider returns an access token that appears to be a JWT, but which is invalid.  Mandatory.  Default: <b>false</b>
<b>max-clock-skew</b>	The maximum time difference between the ALM Octane system and the OIDC provider system in milliseconds. The value can be suffixed with "s", "m", "h", or "d" to indicate that the value is seconds, minutes, hours, or days.  <b>Note:</b> If systems are time-synchronized using NTP, there is no need to set maximum skew time to more than a couple of seconds.  Mandatory.  Default: <b>1s</b>

Setting	Description and usage
<b>oidc</b>	<p>The oidc section contains the following settings.</p> <ul style="list-style-type: none"> <li>• <b>client-id</b> and <b>client-secret</b>. The OIDC client ID and secret to use in your organization's tool for the token exchange. The OIDC client ID and secret should be placed in the Authorization header as Basic:  <code>Authorization: Basic Base64(clientId:clientSecret)</code>  Mandatory.</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• The OIDC client ID is not the same client ID that is used by the tool for authentication.</li> <li>• OIDC client ID and secret differ from: <ul style="list-style-type: none"> <li>◦ The API key used for authentication in the authorization server.</li> <li>◦ The client ID and secret defined in the <b>sso.oauth</b> section because of the different usage scenarios. Client ID and secret from <b>sso.oauth</b> are used by ALM Octane during the SSO authentication flow, while client ID and secret from the <b>token-exchange.oidc</b> section are used by the tool that performs the token exchange.</li> </ul> </li> <li>• <b>authentication-timeout</b>. The federated SSO authentication timeout in seconds.  Mandatory.  Default: <b>10800</b> seconds (3 hours).</li> </ul>
<b>mapping</b>	<p>The mapping section contains the following settings. Only the standard OIDC claims are supported.</p> <ul style="list-style-type: none"> <li>• <b>user-name</b>. Defines the claim in the access token from the authorization server that holds the name of the authenticated API key. This is used for mapping the authenticated API key with its role in ALM Octane.  Mandatory.</li> <li>• <b>session-identifier</b>. Defines the claim in the access token from the authorization server that holds a unique authentication identifier (for example "txn", Transaction Identifier).  Mandatory.  Default: <b>jti</b></li> </ul>

### Logging settings:

Setting	Description and usage
<b>directory</b>	<p>The directory in which to create the SSO log files.  Optional. If the value is empty then the default logging directory will be used.  Default: <b>&lt;log folder&gt;/sso</b></p>

Setting	Description and usage
<b>logging-level</b>	Logging level. Possible values are: <ul style="list-style-type: none"><li>• <b>SEVERE</b></li><li>• <b>INFO</b></li><li>• <b>WARNING</b></li><li>• <b>ALL</b></li></ul> Optional. Default: <b>WARNING</b>

## Configuration tips

- In production systems, only secure configuration (HTTPS) is supported. In staging, we do not recommend using non-secure configuration as the industry standard is to always use secure communication. Non-secure configuration results in poorer client performance, which does not fully represent what will happen in the production environment.
- ALM Octane uses the TLS version 1.2 secure protocol. To configure a secure connection using TLS (SSL), obtain the server certificate issued to the name of this server in java keystore format (.jks) issued to the fully qualified domain name of server. It must contain a private key and the certificate authority that issued it. For details on creating certificates using the Certificate Authority, see [ALM Octane Secure Deployment and Configuration Guidelines](#).  
You then enter certificate details in the section "[Public URL and Server Ports](#)" on [page 48](#).
- When you install a single node configuration for the Jetty server, you need to use the full address to access it. Meaning, if the Jetty server was installed on a machine named **myserver.mydomain.com**, then you access it via: **http[s]://myserver.mydomain.com:<port>** and not via **http[s]://myserver:<port>** if there are client-side DNS shortcuts installed.
- When you install a cluster Jetty server environment, the load balancer and all Jetty nodes should all be accessible from one another. The same rules for accessing the server via the load balancer from the client side apply. Meaning, the full address of the load balancer should be used for access.

## Start the ALM Octane server

When you finish defining your configuration settings as described in ["Configure site settings" on page 37](#), start ALM Octane.

### To start the ALM Octane server:

1. Select **Start > ALM Octane > Start ALM Octane Server**.

Alternatively, start the **ALM Octane** service.

The installation is complete when the "Server is ready!" message is shown in the **C:\Program Files\octane\log\wrapper.log** file. If you do not see the "Server is ready!" message, correct the errors shown in the log.

2. You are now ready to:

- **Single-node configuration:** Log in and create additional users. For details, see ["Log in to ALM Octane" on the next page](#).

Check connectivity by logging in, after initializing the first node and before installing the remaining cluster nodes.

- **Cluster configuration:** Optional.

For details on installing on a cluster, see ["Cluster installation flow" on page 17](#).

### Next steps:

- ["Log in to ALM Octane" on the next page](#)
- ["Cluster installation flow" on page 17](#)

# Log in to ALM Octane

This section describes how to log into ALM Octane.



**Tip:** When you first start using ALM Octane, you automatically receive a Trial license which gives you a 90-day trial for 100 users. For details, see [Trial license](#) in the ALM Octane Help Center.

## To log into ALM Octane:

1. In a browser, go to `<serverURL>:<serverport>/ui`.

Make sure to specify a fully-qualified domain name for the server. The name must include at least one period. Do not specify an IP address.

**Cluster configuration:** Use the load balancer URL.

2. Log in with the site admin user name and password you provided in the `octane.conf` file using settings **site-administrator name** and **password**.



**Note:** Errors might be listed even if the ALM Octane server initializes and starts. If you encounter problems initializing ALM Octane, check for errors in the log files.

## Next steps:

- **Cluster configuration:** If you successfully installed and logged into ALM Octane on the first cluster node, continue installing on additional cluster nodes. See ["Cluster installation flow" on page 17](#).
- Set configuration parameters, such as `FORGET_USER_ON_DELETE` and `SMTP_NOTIFICATION_SENDER_EMAIL`. See [Configuration parameters](#) in the ALM Octane Help Center.
- Create spaces. See [Create a space](#) in the ALM Octane Help Center.
- Once you have logged on as the space admin, you can create other users and workspaces. See [Users](#) and [Create workspaces](#) in the ALM Octane Help Center.



# Install ALM Octane using a Docker image

This section describes how to install ALM Octane using a Docker image.

**Note:** The ALM Octane Docker container is based on a Linux image. This section relates to running this container on a Windows host.

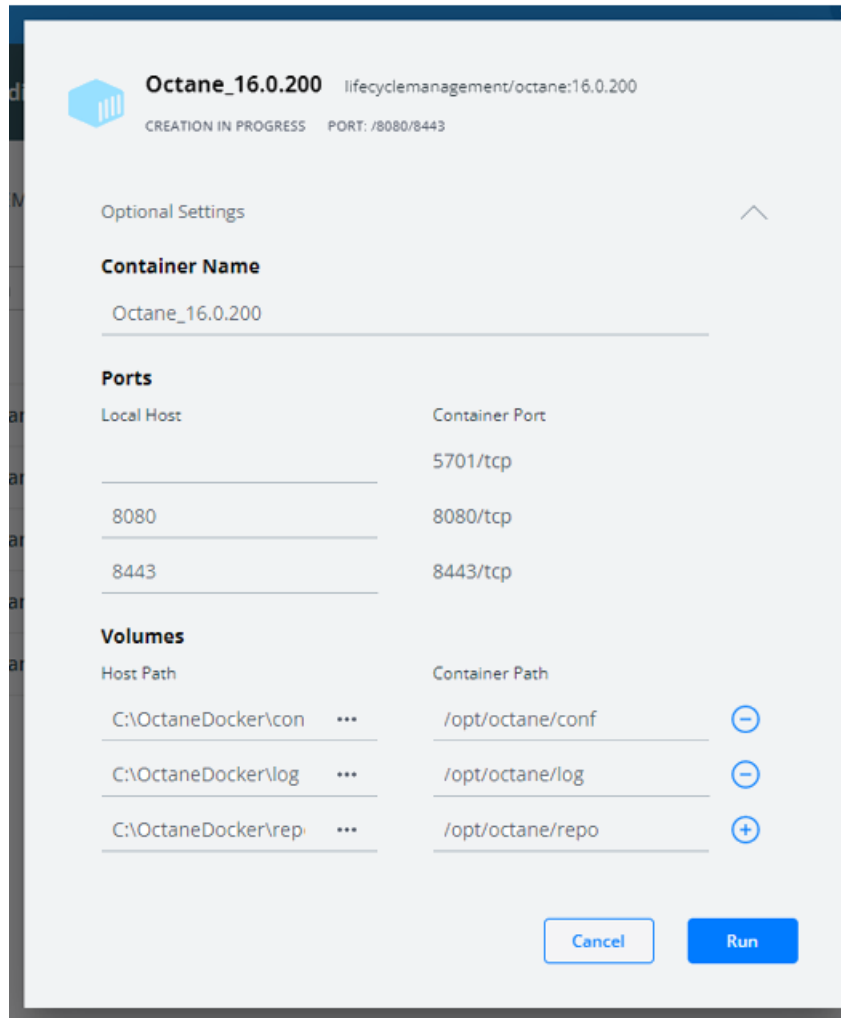
1. Download and install the latest version of Docker Desktop.
2. In the Docker Hub, search for **Octane**.
3. Select **lifecyclemangement/octane**. The description should say: The official repository for ALM Octane.
4. Select **Tags**.
5. Choose the ALM Octane version you want to install, and copy the download command.

**Note:** The list you see includes both SaaS versions and on-premises versions of ALM Octane, but only on-premises versions are supported. Select an on-premises version now.

6. In a command line, run the command you copied.
7. In Docker Desktop, select **Images** in the left pane.
8. Locate the ALM Octane version you want to install. To configure the container, click **RUN**.
9. Open the **Optional Settings**, and enter the following:

# Installation Guide for Windows

## Install ALM Octane using a Docker image



- In **Container name**, enter a name of your choice.
- In **Ports**, enter 8080 to use HTTP, or 8443 to use HTTPS.
- In **Volumes**, enter the following:

Host path	Container path
C:\OctaneDocker\conf	opt/octane/conf
C:\OctaneDocker\log	opt/octane/log
C:\OctaneDocker\repo	opt/octane/repo

10. Click **Run** to execute the Docker image for the first time.

The run fails with errors, because ALM Octane has not yet been configured.

11. Open the **octane.conf** file located in **C:\OctaneDocker\repo\conf-discover\octane.conf**.
12. Configure ALM Octane as described in ["Configure site settings" on page 37](#).

**Note:** If you want to use resources from your local machine instead of localhost, use host.docker.internal.

13. When you are done, run the container from **Containers/Apps**.
14. Check for errors in the **wrapper.log** and **octane.log** files, in the folder **C:\OctaneDocker\log**.
15. ALM Octane is now ready for use.

# Management

Here are some management tasks you may have to perform during or after installation.

**Note:** In addition to these management tasks, you can also set configuration parameters to define how your site operates. Configuration parameters for the site are set using Settings. See [Configuration parameters](#) in the ALM Octane Help Center.

This section includes:

## Start the ALM Octane server manually

If you need to start the ALM Octane server manually, perform the following.

**To start (or restart) the ALM Octane server:**

Select **Start > ALM Octane > Start ALM Octane Server**

The service runs in the background.

**To start (or restart) ALM Octane in a cluster configuration:**

All nodes must be restarted.

 **See also:**

- ["Management" above](#)

## Handle database-related issues

This topic provides instructions for handling database-related management tasks.

This section includes:

- ["Change site schema settings and reinitialize" below](#)
- ["Update database password in ALM Octane site schema and configuration files" on the next page](#)

## Change site schema settings and reinitialize

If you need to make changes to the site schema settings, make the changes in the **octane.conf** file.

### To change site schema settings and reinitialize:

1. Obtain the names of the indexes related to your instance of ALM Octane in the **sharedspace\_logical\_name.txt** in the **C:\Program Files\octane\server\conf\** folder.
2. Delete the database site schema.
3. Delete the repository.
4. Delete the **mqm\_<sp\_logical\_name>** indexes from Elasticsearch. From the command prompt on the ALM Octane server, run:

```
curl -XDELETE 'http://<server address>:9200/mqm_<sp_logical_
name>/'
```

5. Select **Start > ALM Octane > Start ALM Octane Server**.

## Update database password in ALM Octane site schema and configuration files

If you change your database password, you can use the database password update tool to update the database password in ALM Octane's site schema, and in the octane.conf configuration files. Note that this does not update the database user's password, but only ALM Octane's configuration.

**Note:** The tool operates offline. Credential outputs are disabled for security.

1. Stop the ALM Octane server.

After stopping the server, wait 30 seconds before running the tool. The cluster is considered offline when there is no activity from any node for 30 seconds.

2. Run the following command as an administrator on your ALM Octane server:

```
\opt\octane\install\updatedbcreds.bat
```

3. Enter values as described in the sections below.
4. When you are done, start the ALM Octane server.

### Usage

The tool can operate in 2 modes: file, or interactive.

```
updatedbcreds.bat <-m mode> <-f path | -t target>
```

Where:

- mode = {file | interactive}
- target = {admin | user}
- path = valid absolute or relative path to file

**File.** If mode is set to file, use -f to specify the path to the password definition file. Credentials are taken from the provided file.

**Interactive.** If mode is set to interactive, use -t to specify the target whose password you want to change - either admin or user. You then enter credentials interactively.



**Example:** If you want to update the db.admin-user in the config file, the target should be **admin** (in Interactive mode).

If you want to update the db.<db-vendor>.app-user-name in the config file, the target should be **user** (in Interactive mode).

## File mode

You can use the CLI in file mode, which allows granular definitions for admin, user, or space passwords.

Using a tool in file mode looks like this:

```
updatedbcreds.bat -m file -f /path/to/definition.json
```

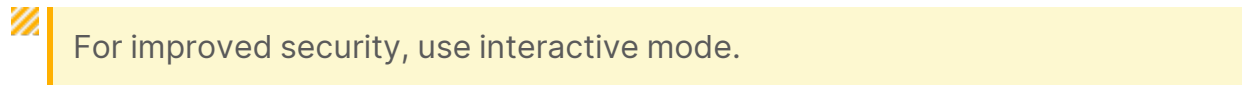
This is done using a JSON password definition file, in the following format:

```
```json
{
  "admin" : {
    "password" : "PasswordForAdminUser"
  },
  "appUser" : {
    "password" : "PasswordForAppUser"
  },
  "spaces": {
    "default_shared_space": {
      "password": "PasswordForSpecificSpace"
    }
  }
}
```

In SQL Server, you can delete the **spaces** section. In this case all spaces get the appUser password.



**Caution:** Before the tool runs, your file contains passwords in clear text. It is your responsibility as administrator to secure the file according to your organization's policies. The tool encrypts the file when running. The tool can read the encrypted password if you want to rerun the tool.

 For improved security, use interactive mode.

### Interactive mode

In interactive mode you update only the admin or user password. This is useful when you do not need extensive password definition and just want to change a password for a single user.

Using a tool in interactive mode looks like this:

```
updatedbcreds.bat -m interactive -t admin
```

Enter the following:

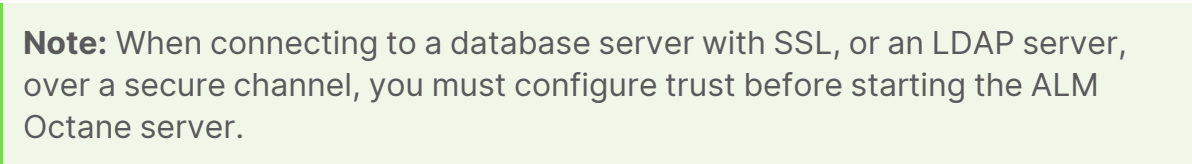
- New password for ADMIN: Enter a new password for admin user. Output is disabled.
- DB authentication username: Enter a user for CLI database connection. Output is disabled.
- DB authentication password: Enter a password for CLI database connection. Output is disabled.

### See also:

- ["Management" on page 68](#)

## Configure trust on the ALM Octane server

Configure trust on the ALM Octane server when you connect to any remote server (such as a database server, an LDAP server, license sharing with ALM, and so on) over a secure channel.

**Note:** When connecting to a database server with SSL, or an LDAP server, over a secure channel, you must configure trust before starting the ALM Octane server.



## To configure trust:

1. Obtain the certificate of the root and any intermediate Certificate Authority that issued the remote server certificate.
2. Import each certificate into the ALM Octane java truststore using a keytool command.

- Locate your **<java\_home>** folder. One way to check the location of the **<java\_home>** folder is to check the environment information settings in the **C:\Program Files\octane\log\wrapper.log** file.

**Example: C:\Program Files\java\<jdkversion>\jre**

- Locate your keystore **cacerts** file, which is usually here: **<java\_home>\jre\lib\security\cacerts**
- Import each certificate.

**Example:**

```
cd <java_home>\bin  
  
.\keytool -import -trustcacerts -alias <CA> -file <path to the  
CA certificate file> -keystore ..\lib\security\cacerts
```

3. If the ALM Octane service is running, restart it.



**Tip:** For general details on configuring HTTPS, see "Secure configuration and deployment" in the [ALM Octane Secure Deployment and Configuration Guidelines](#).

## Next steps:

- ["Management" on page 68](#)

# Using exception files for manual database changes

This topic provides instructions for defining exception files. Use exception files if the organization's DBA added objects to database schemas, such as tables,

indexes, stored procedures, columns, or other objects.

This section includes:

- ["Overview" below](#)
- ["Define exception files" below](#)
- ["Set up use of the exception file" on page 76](#)

## Overview

Exception files instruct ALM Octane to ignore any errors issued because of manual additions to the database schema. These errors would typically stop the installation or upgrade process.

You can use exception files to ignore errors for extra tables, views, columns, and sequences. For any other problem, consult with your database administrator.



**Caution:** Using the exception file to ignore errors for objects that are added manually to the schema may compromise stability and the validity of the database user schema.

You can use the exception files during a new ALM Octane installation, when upgrading, and when creating a space.

## Define exception files

Define exception files before installation, before upgrading, or before you create the new spaces.

### To define exception files:

1. Copy both of the **mqm\_exception.xml** files from the ALM Octane installation directories. You can rename them.
2. Locate the MQM\_EXCEPTIONS part of the file.

```
<MQM_EXCEPTIONS>  
  <exceptions>
```

```
        <declaration>
            <!--<object pattern="TABLE_1_EXAMPLE" type="missing"
/>-->
            <!--<object pattern=" TABLE_1_EXAMPLE" type="extra"
/>-->
        </declaration>
    </exceptions>
</MQM_EXCEPTIONS>
```

3. Change the <declaration> to one of the following. Add as many declarations as you need.

- TableMissing
- ViewMissing
- ColumnMissing
- ConstraintMissing
- IndexMissing
- PartitionFunctionMissing
- PartitionSchemeMissing
- ProcedureMissing
- SequenceMissing
- TriggerMissing

4. For each object pattern, you can specify one of the following types:

missing	The object is needed but is missing.
extra	The object is extra because it was created after ALM Octane installation or before upgrading.

### Examples

- For an extra table:

```
<TableMissing>
    <object pattern="MY_Table" type="extra"/>
```

```
</TableMissing>
```

- For an extra view:

```
<ViewMissing>  
    <object pattern="MY_VIEW" type="extra"/>  
</ViewMissing>
```

- For an extra column:

```
<ColumnMissing>  
    <object pattern="MY_COLUMN" type="extra"/>  
</ColumnMissing>
```

- For an extra sequence:

```
<SequenceMissing>  
    <object pattern="MY_SEQUENCE" type="extra"/>  
</SequenceMissing>
```

## Set up use of the exception file

This topic explains how to use the exception file when installing ALM Octane, when upgrading, or when creating a new space.

### Use of the exception files during first-time installation

You can use exception files when installing ALM Octane using existing schemas/databases instead of having ALM Octane create new schemas for you. This is the **FILL\_EXISTING** installation option and it is set in the **octane.conf** file.

1. During installation, when configuring the **octane.conf** file in the configuration folder, add these two settings using an editor:

<b>MqmExceptionsSiteAdminPath</b>	The exception file for the site. <b>C:/temp/site_admin/mqm_exception.xml</b>
-----------------------------------	---------------------------------------------------------------------------------

<b>MqmExceptionsSharedSpacePath</b>	The exception file for the default space. <b>C:/temp/shared_space/mqm_exception.xml</b>
-------------------------------------	--------------------------------------------------------------------------------------------

2. Continue installing.
3. Check that the ALM Octane Server is up and that you have proper access to the site and the default space.

## Use of the exception files when upgrading

You can use exception files when upgrading ALM Octane.

After installation, the exception files are copied to the repository folder. So when upgrading, modify the copies of the exception files in the repository folder instead of the files in the configuration folder.

1. During the upgrade, when configuring the **octane.conf** file in the repository folder, add or modify these two settings using an editor:

The exception file for the site	<b>C:\Program Files\octane\repo\storage\schema\maintenance\exceptions\site_admin\mqm_exception.xml</b>
---------------------------------	--------------------------------------------------------------------------------------------------------

The exception file for the new space	<b>C:\Program Files\octane\repo\storage\schema\maintenance\exceptions\shared_space\mqm_exception.xml</b>
--------------------------------------	----------------------------------------------------------------------------------------------------------

2. Continue upgrading.
3. Check that the ALM Octane Server is up and that you have proper access to the site and the default space.

## Use of the exception files when creating a space

ALM Octane processes the exception files also when adding new spaces.

After installation, the exception files are copied to the repository folder.

Before adding a new space, modify the copies of the exception files in the repository folder instead of the files in the configuration folder.

1. Add exceptions as necessary to the exception files using an editor:

The exception file for the site	<b>C:\Program Files\octane\repo\storage\schema\maintenance\exceptions\site_admin\mqm_exception.xml</b>
The exception file for the new space	<b>C:\Program Files\octane\repo\storage\schema\maintenance\exceptions\shared_space\mqm_exception.xml</b>

2. In ALM Octane Settings area, add the space using an existing schema. For details, see [Create a space](#) in the ALM Octane Help Center.
3. Check that you have proper access to the space.

#### See also:

- ["Configure site settings" on page 37](#)
- ["Management" on page 68](#)

## Advanced ALM Octane server configuration

This section describes advanced configuration tasks for the ALM Octane server.

### Configure secure database access

This section describes how to configure a secure connection from the ALM Octane server to the database server. The secure connection is protected with SSL/TLS for encryption and authentication.

This section includes:

- ["Defining the connection-string for secure database access" on the next page](#)
- ["To configure a secure database connection for a previously-unsecured database " on page 80](#)

- ["To configure a secure database connection for a new ALM Octane installation" on the next page](#)

## Defining the connection-string for secure database access

### SQL Server

SQL Server Scenario	Instructions
<b>SSL/TLS is required</b>	<p>Add the encryption method to the end of the <b>ConnectionString</b> value.</p> <p><b>jdbc:sqlserver://&lt;server&gt;:&lt;port&gt;;encrypt=true;trustServerCertificate=true</b></p>
<b>SSL without certificate validation</b>	<p>When using SSL, disable validation of the certificate sent by the database server. Add the encryption method to the end of the <b>ConnectionString</b> value, and apply the certificate into the java certs file located under <b>&lt;JAVA_HOME&gt;\jre\lib\security\certs</b>.</p> <p><b>jdbc:sqlserver://&lt;server&gt;:&lt;port&gt;;encrypt=true;trustServerCertificate=false;trustStore=&lt;Java Certs file&gt;;trustStorePassword=&lt;JKS password&gt;</b></p>

### Oracle

Oracle scenario	Instructions
<b>SSL/TLS required</b>	<p>To configure a secure connection from the ALM Octane server to the database server using SSL or SSO, refer to the section <a href="#">"Using SSL/SSO in Oracle (optional)" on page 41</a>.</p> <p>The connection string should include the port defined in the Oracle database as the port for SSL connections. The protocol should be set to TCPS:</p> <pre>connection-string = "jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=&lt;hostname&gt;)(PORT=&lt;ssl port&gt;)) (CONNECT_DATA=(SERVICE_NAME=&lt;ORA_SERVICENAME&gt;)))"</pre>

## To configure a secure database connection for a previously-unsecured database

This step provides instructions for configuring the site schema connection.

Skip this section if you have a separate database server for your workspaces and you only want a secure connection to that database.

This section is relevant if the database server that was configured for a secure connection contains your site schema.

1. Edit the **octane.conf** file. The default location is **/opt/octane**):
  - a. Set the value of **site-action** to **CONNECT\_TO\_EXISTING**:

```
site-action=CONNECT_TO_EXISTING
```
  - b. Edit the line with **connection-string**.
2. If SSL/TLS is required, make sure the trust on the ALM Octane server has been established. For details, see ["Configure trust on the ALM Octane server" on page 72](#).
3. Run the service to start the ALM Octane server.

```
systemctl start octane
```

## To configure a secure database connection for a new ALM Octane installation

1. After installing ALM Octane, start the server:

```
systemctl start octane
```

2. In the Database Server step, select the **connection-string** option and set the values for your database.
3. Make sure the trust on ALM Octane the ALM Octane server has been established. For details, see ["Configure trust on the ALM Octane server" on page 72](#).



 **See also:**

- ["Management" on page 68](#)

# Uninstall

To uninstall the ALM Octane server, use the uninstall feature from the Windows Control Panel.

The uninstall process does not delete the repository, log, and configuration directories, in case you want to reinstall. Delete them if necessary.

## See also:

- ["Installation" on page 34](#)