



ALM Octane

Software Version: 12.60.21

Installation Guide for Windows

Go to **HELP CENTER ONLINE**
<http://admhelp.microfocus.com/octane/>

Legal Notices

Disclaimer

Certain versions of software and/or documents (“Material”) accessible here may contain branding from Hewlett-Packard Company (now HP Inc.) and Hewlett Packard Enterprise Company. As of September 1, 2017, the Material is now offered by Micro Focus, a separately owned and operated company. Any reference to the HP and Hewlett Packard Enterprise/HPE marks is historical in nature, and the HP and Hewlett Packard Enterprise/HPE marks are the property of their respective owners.

Warranty

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

Restricted Rights Legend

Contains Confidential Information. Except as specifically indicated otherwise, a valid license is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2016-2018 Micro Focus or one of its affiliates.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

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

Comodo Code Signing Certificate

The code signing certificate for ALM Octane was changed from Verisign to Comodo starting on January 1, 2017.

If you are installing this product on a computer with an older version of Windows, or on a computer without automatic Windows updates, the Comodo root certificate may not automatically be included as a trusted root certificate.

In such cases, we recommend manually configuring Comodo as a trusted root certificate.

For more details, see: <https://technet.microsoft.com/en-gb/library/dn265983.aspx>.

Contents

ALM Octane	1
Architecture	5
Basic configuration	5
Enterprise configuration	6
Components	8
Installation types	11
Licensing flow	11
Overview	12
Request a trial	12
Using Pro Edition	12
Install a license	13
Installation flow	13
Prerequisites	13
Deployment	14
Configuration	14
Initialization	14
Verify and log in	14
Cluster configuration (optional)	15
Prerequisites	15
System requirements	15
Checklist	18
Permissions	22
Installation	23
Deploy ALM Octane	25
Overview	25
Prerequisites	25
Deploy	25
Deploy in cluster environment	26
Configure initial site settings	27
Overview	27
Database server settings	27
Oracle server settings	30
SQL Server settings	30
Site actions	30
Space settings	31
Elasticsearch settings	32
Site admin credential settings	33
Repository settings	33
Additional settings	34
Configure other settings	34

Overview	34
Rules for editing the octane.yml file	34
General server settings	35
LDAP settings	36
License settings	41
Oracle settings	42
Cluster settings	42
ALM Octane service provider (SP) settings	43
Update settings	49
How to update settings	49
Initialize the ALM Octane server	49
Log in to ALM Octane	50
Cluster installation (optional)	50
Overview	51
Install ALM Octane in a cluster configuration	52
Upgrade	54
Before you upgrade	55
Deploy	57
Configure initial settings	57
Configure other settings	58
Upgrade	72
Configure and upgrade cluster nodes	72
Upgrade spaces in ALM Octane	73
Restart all Jetty servers	73
After the upgrade	74
Bulk update data access control	74
Rollback	74
After the upgrade's setup validation phase	75
After site schema has been upgraded	75
After space schema has been upgraded	76
After upgrade completed	76
After upgrading cluster nodes	77
Management	77
Start the ALM Octane server manually	78
Handle database-related issues	78
Change site schema settings and reinitialize	78
Configure trust on the ALM Octane server	79
Configure trust	79
Configure a secure connection to the ALM Octane server (Jetty)	80
Configure the connection	80
Limitations	80
Using exception files for manual database changes	81
Overview	81

Define exception files	81
Set up use of the exception file	83
Best practices	84
Best practices: Deploying ALM Octane	85
Overview	85
Architecture	85
General guidelines	85
Minimal and suggested requirements	86
Best practices: Backing up ALM Octane data	86
Overview	86
The process	87
Best practices	88
Best practices: Maintenance	88
Overview	89
Periodic maintenance	89
Disaster recovery	89
Best practices: Setting up spaces and workspaces	90
Overview	90
Planning how to set up spaces	91
Planning how to set up workspaces	93
Uninstall	95
Send Us Feedback	97

Architecture

You can set up 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.

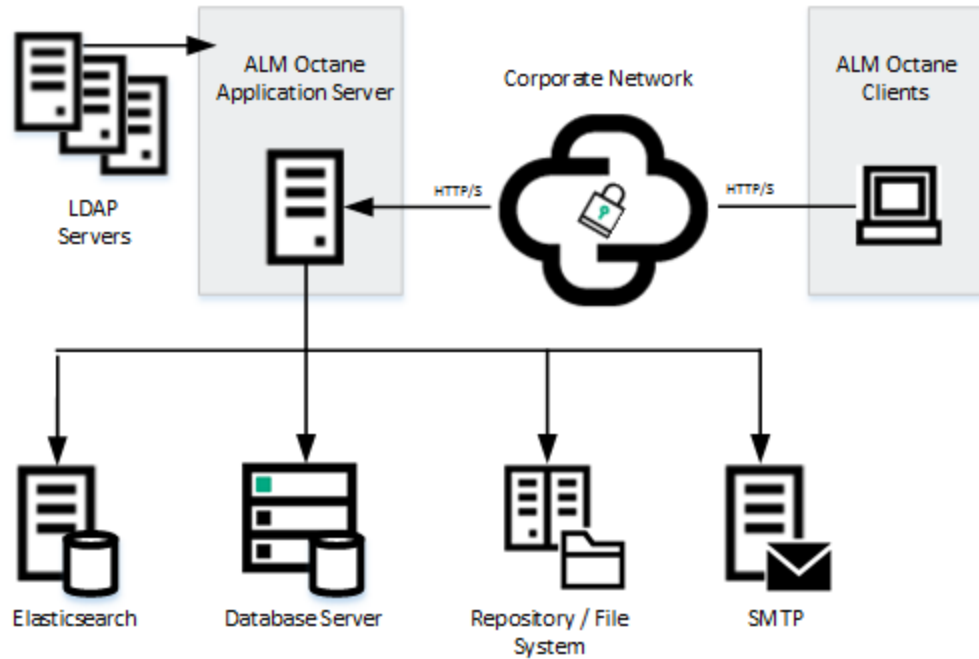
- ["Basic configuration" below](#)
- ["Enterprise configuration" on the next page](#)
- ["Components" on page 8](#)

Basic configuration

The following diagram illustrates the system architecture of a single-node configuration.

Components in grey are Micro Focus products.

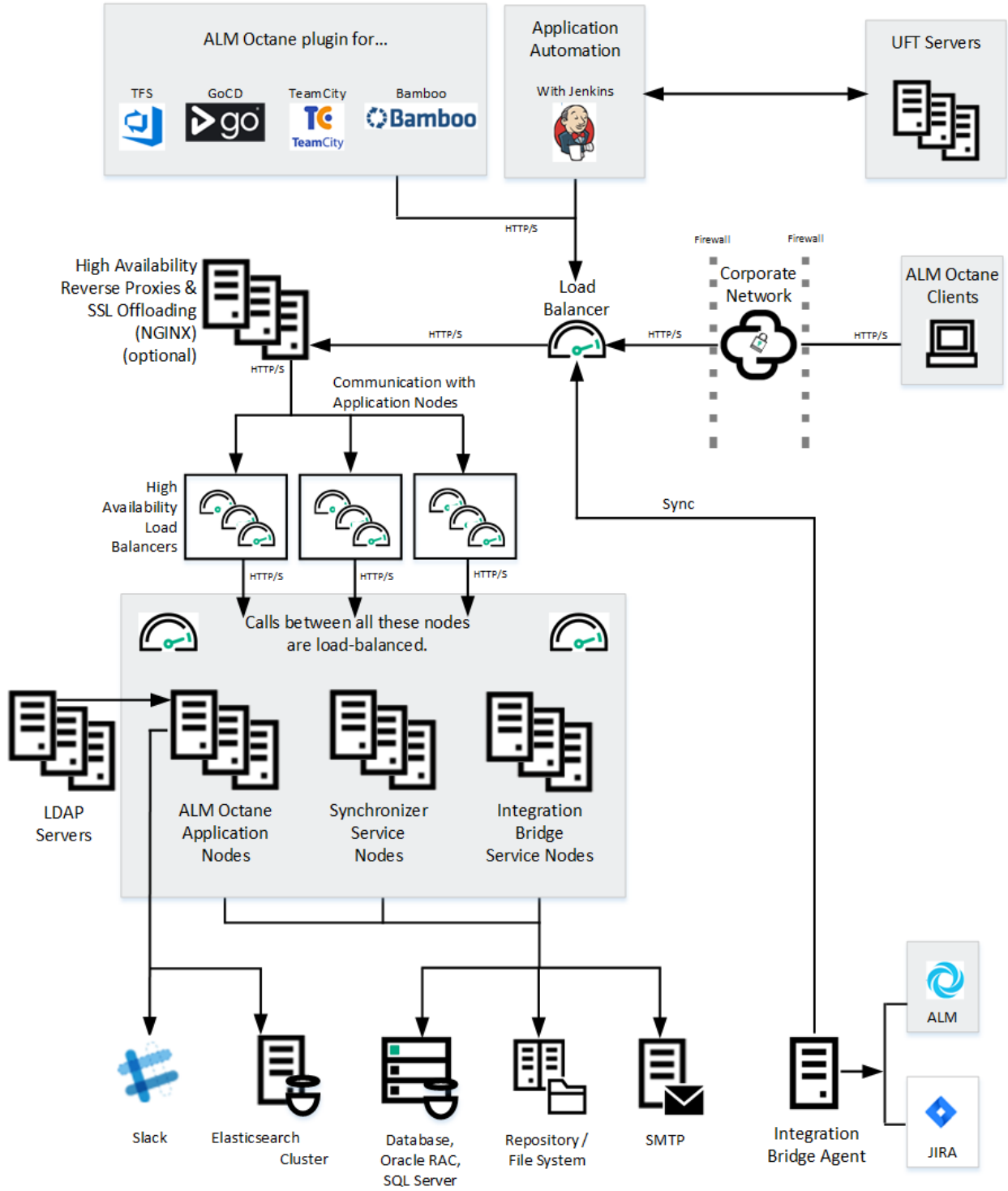
Note: The ALM Octane, database, and Elasticsearch servers should each reside on separate machines.



Enterprise configuration

The following diagram illustrates the system architecture of an enterprise, cluster configuration:

Components in grey are Micro Focus products.



Components

Components	Description
ALM Octane clients	The clients communicate with the ALM Octane server over HTTP/S.
Integration bridge and external sources	<p>Enterprise configuration: The integration bridge enables ALM Octane to integrate with external applications ("off-organization" communication). This is generally optional, but required for synchronization. Also used for Trigger Webhook rules to an endpoint URL, SaaS deployments, and for communication between Micro Focus SaaS and an on-premises deployment.</p>
ALM Octane Server application nodes	<p>Client requests from ALM Octane are dispatched to the deployed application.</p> <div style="border: 1px solid green; background-color: #e6f2e6; padding: 5px;"><p>Note: The ALM Octane, database, and Elasticsearch servers should each reside on separate machines.</p></div>
ALM Octane application additional cluster (sync) nodes	<p>Cluster configuration: 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."</p> <ul style="list-style-type: none">• All nodes must have access to the database server on which the site database schema resides.• All nodes must have access to the repository. Generally, the repository will be located on an NFS or SAN server.• All nodes must have access to each other.
Integration bridge service nodes	The service handles communication between the Integration Bridge and Synchronizer.
Synchronizer service nodes	The service nodes handle synchronization between ALM Octane and ALM or JIRA.
Repository / File system	<p>Stores all files to be used by all the projects in the system, such as templates and attachments.</p> <p>Cluster configuration: 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.</p>

Components	Description
Database server	<p>A relational database management system, either Oracle RAC or Microsoft SQL Server.</p> <p>The database server stores the following schemas:</p> <ul style="list-style-type: none">• Space schema. All space information, such as workspaces, users, and roles..• Site schema. Stores all site-related information, such as database servers, cluster nodes, the SMTP servers, and configuration. <p>This server can be shared with other applications with the following constraints:</p> <ul style="list-style-type: none">• The database must be able to sustain the load of all the applications.• Future versions of ALM Octane might require a database upgrade. This may necessitate migration of data if other applications sharing the same database will not support the database version that ALM Octane requires. <p>Note: The ALM Octane, database, and Elasticsearch servers should each reside on separate machines.</p>

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"> • The database must be able to sustain the load of all the applications. • Future versions of ALM Octane might require a database upgrade. This may necessitate migration of data if other applications sharing the same database will not support the database version that ALM Octane requires. <div style="border-left: 2px solid green; padding-left: 10px; margin: 10px 0;"> <p>Note: 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> <ul style="list-style-type: none"> • For the supported version, see the requirements for Database and Elasticsearch. • For details on installing Elasticsearch, see knowledge base article KM02494295. • For details on upgrading to a new Elasticsearch version, see knowledge base article KM03207448.
Load balancer	<p>Cluster configuration: 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>Cluster configuration: 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>Cluster configuration: 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>Enterprise configuration: You can integrate ALM Octane with a Jenkins CI server using the Application Automation Tools Plugin on your CI server.</p>

Components	Description
TeamCity, Bamboo, or TFS server (with ALM Octane plugin)	Enterprise configuration: You can integrate ALM Octane with a TeamCity, Bamboo, or TFS CI server using the ALM Octane CI Plugin on your CI server.
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.
Micro Focus testing tools: LeanFT, UFT, LoadRunner, StormRunner Functional, StormRunner Load, Performance Center	You can integrate ALM Octane with Micro Focus testing tools. For details, see the topic on ALM Octane DevOps integrations in the <i>ALM Octane Help Center</i> .

 **See also:**

- ["Prerequisites" on page 15](#)
- ["Installation types" below](#)
- ["Installation flow" on page 13](#)
- ["Installation" on page 23](#)
- ["Deploy ALM Octane" on page 25](#)

Installation types

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

Type	Description
This Windows Installation	Instructions for installing on: <ul style="list-style-type: none">• A single node.• A cluster configuration. For details, see "Installation" on page 23 .
Upgrade	For details, see "Upgrade" on page 54 .

 **See also:**

- ["Prerequisites" on page 15](#)
- ["Deploy ALM Octane" on page 25](#)
- ["Configure initial site settings" on page 27](#)
- ["Configure other settings" on page 34](#)

Licensing flow

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

In this topic:

- ["Overview" below](#)
- ["Request a trial" below](#)
- ["Using Pro Edition" below](#)
- ["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, Pro, and Team Editions. *Help Center*. For details, see topic about ALM Octane editions in the *ALM Octane Help Center*.

Request a trial

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

When you install ALM Octane, you can choose between an Enterprise Edition or Team Edition trial. For details on selecting your trial, see [License settings](#).



Caution: If you want to use the Pro Edition, choose the Enterprise Edition for your trial. Make sure to follow the instructions under ["Using Pro Edition" below](#).

You cannot switch between editions once configuration is done, so choose your trial and editions carefully. If you chose the wrong edition, re-install ALM Octane.

Using Pro Edition

There is no Pro Edition trial. To work with Pro Edition:

1. Install ALM Octane and select 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" on the next page](#).

Install a license

After you install and configure your trial instance of ALM Octane, you can purchase licenses for Enterprise, Pro, or Team 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.

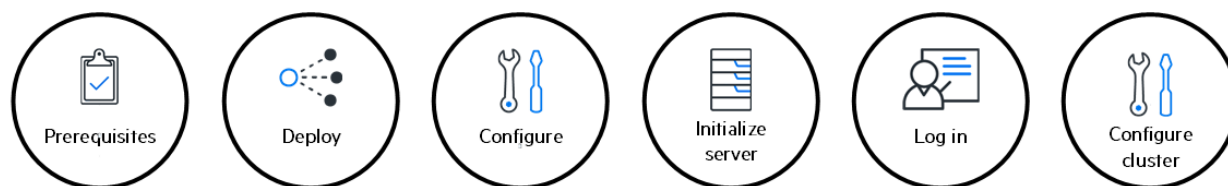
To learn more, see the topic about managing licenses in the *ALM Octane Help Center*.

Next steps:

- ["Installation flow" below](#)

Installation flow

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



In this topic:

- ["Prerequisites " below](#)
- ["Deployment " on the next page](#)
- ["Configuration " on the next page](#)
- ["Installation flow" above](#)
- ["Initialization " on the next page](#)
- ["Verify and log in " on the next page](#)
- ["Cluster configuration \(optional\) " on page 15](#)

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 the next page](#).

Note: We recommend you review security considerations in the knowledge base article [KM02707977](#). This article 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:\octane**.

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

For details, see ["Deploy ALM Octane" on page 25](#).

Configuration

Configure ALM Octane by editing these files with your site's settings:

- **setup.xml** for initial configuration
- **octane.yml** for ongoing configuration

The path to these files is **C:\octane\conf**.

For details, see ["Configure initial site settings" on page 27](#) and ["Configure other settings" on page 34](#).

If you have previously installed ALM Octane on this machine, select **Start > ALM Octane > Update ALM Octane Settings**. For details, see ["Update settings" on page 49](#).

Initialization

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

This also starts the server.

For details, see ["Initialize the ALM Octane server" on page 49](#).

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 50](#).

Cluster configuration (optional)

After starting the server on the first machine, configure and initialize each additional cluster node. For details, see ["Cluster installation \(optional\)" on page 50](#).

Prerequisites

Verify that your system meets the requirements listed below, and that permissions are assigned as necessary..

For security requirements, see [Software Self-solve knowledge base article KM02707977](#).

In this topic:

- ["System requirements" below](#)
- ["Checklist" on page 18](#)
- ["Permissions" on page 22](#)

System requirements

Hardware

Component	Type	Version
Server operating system	CentOS	6.5 or later We strongly recommend 7.2 and later.
	Suse	12 with SP1 or SP2
	Red Hat Enterprise Linux (RHEL)	6.5 or later We strongly recommend 7.2 and later.
Browser	Chrome (recommended)	Chrome: The two latest versions Chrome for business
	Firefox (recommended)	Firefox: The two latest versions ESR: 52
	Internet Explorer	11
	Apple Safari	10, 11

Component	Type	Version
JDK		Open/Oracle JDK 8 Java 8 only. Make sure the latest security updates are installed on the ALM Octane server at all times.

Software

Component	Type	Version
Server operating system	Windows	2012, 2016
Browser	Chrome (recommended)	Chrome: The two latest versions Chrome for business
	Firefox (recommended)	Firefox: The two latest versions ESR: 52
	Internet Explorer	11
	Apple Safari	10, 11
JDK		Open/Oracle JDK 8 Java 8 only. Make sure the latest security updates are installed on the ALM Octane server at all times.

Database and Elasticsearch

Component	Type	Version
Database	Oracle	12C Standard or Enterprise edition, with character set AL32UTF8
	SQL Server	2016, 2014 or 2012 SP3 Case-insensitive collations only.

Component	Type	Version
Elasticsearch	N/A	5.6.X <ul style="list-style-type: none">For details on installing Elasticsearch, see knowledge base article KM02494295.For details on upgrading to a new Elasticsearch version, see knowledge base article KM03207448.


Integrations


Installation, setup, and synchronization


Component	Version
Cloud environments	Amazon Web Services (AWS) Microsoft Azure
LDAP Server	Active Directory, or any LDAP provider supporting the LDAP3 protocol
Synchronizer	Synchronizer version must match your ALM Octane version. For installation details see Synchronizer installation .
JIRA synchronization	JIRA 7.2.8 - 7.11.x
ALM/Quality Center synchronization	ALM/Quality Center 12.60 patch 1, 12.55, 12.53, 12.50, 12.21, 12.01 patch 1 and later
ALM/Quality Center license sharing	ALM/Quality Center 12.55, 12.53 (all patch levels), 12.21 patch 6 Note that 12.53 versions require a hotfix .
Upgrade path	Only from 12.53.20




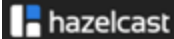
Checklist

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

Category	Tell us...	Your answer...
	On which machine will you be installing ALM Octane?	
	Does the machine have a Quad Core AMD64 processor or equivalent x86-compatible processor?	
	How much memory does the machine have? You need a minimum of 8 GB. Contact customer support for site-specific recommendations.	
	Does the machine have a minimum of 8 GB free disk space? Contact customer support for site-specific recommendations.	
	What Microsoft Windows operating system is on the machine?	
	What is the user name and password you will use for the installation user?	
	Are your browsers and screen resolutions compatible with ALM Octane?	
	On-premises installation of ALM Octane supports only English characters for the names of schemas, operating systems, users, and so on. Did you check?	

Category	Tell us...	Your answer...
 <p>Elasticsearch enables trend reporting and search functionality in ALM Octane.</p>	<p>What Elasticsearch version matches ALM Octane requirements?</p>	
	<p>Do you need to download Elasticsearch?</p> <p>You can download Elasticsearch from https://www.elastic.co/downloads/past-releases/elasticsearch-5-6-5.</p>	
	<p>Did you check Software Self-solve knowledge base articles?</p> <ul style="list-style-type: none"> • Elasticsearch installation and configuration: KM02494295 • Upgrading to a newer Elasticsearch version: KM03207448 	
	<p>On which machine is Elasticsearch installed?</p>	
	<p>What is the Elasticsearch port? Default: 9300</p> <p>You can modify the port in the ConnectionString field in setup.xml.</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>Was Elasticsearch configured according to ALM Octane requirements? For details, see Database and Elasticsearch.</p>	
	<p>Is the Elasticsearch accessible from the ALM Octane server?</p>	

Category	Tell us...	Your answer...
	Does your Oracle version match ALM Octane requirements?	
	On which machine is the database installed?	
	What is the Oracle database port? Default: 9300 You can modify the port in setup.xml .	
	Did you make sure that the port for outbound communication to Oracle is open? By default, outbound ports are open.	
	What is the URL for Java Database Connectivity (JDBC) for your database?	
	What is the database admin's user name and password?	
	Does the database admin have the necessary permissions? See " Permissions " on page 22.	
	What table space and temporary table space can be used?	
	Did the DBA add any objects to the schemas? If so, create an exception file before installing. For details, see " Using exception files for manual database changes " on page 81.	

Category	Tell us...	Your answer...
	<p>Does your SQL Server version match ALM Octane requirements?</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"> • What is the SQL Server database port? Default: 1433 • What is the SQL Server instance name? 	
	<p>What is the database admin's user name and password?</p>	
	<p>Does the database admin power user have the necessary permissions? See "Permissions" on the next page.</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 "Using exception files for manual database changes" on page 81.</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? For details, see JDK.</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 octane.yml.</p>	
	<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 hazelcast.xml.</p>	

Permissions

File system

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

Oracle database

These are the permissions you will define for the user you will specify in the **DBAdminUser** setting in the **setup.xml** file. For details, see ["DBAdminUser" on page 28](#).

Permissions vary depending how you work with ALM Octane and how you want to install.

Do you want ALM Octane to create schemas, objects, and tables during the installation?

Yes	<p>Provide ALM Octane with an Oracle power user with the following admin privileges, so that ALM Octane can create site and space schemas, and objects, automatically during the installation.</p> <ul style="list-style-type: none">• 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. <p>If the database at your site is managed by database administrators, and ALM Octane is not authorized to create its own schemas, this power user can be created temporarily, for installation purposes only. You can remove this user if:</p> <ul style="list-style-type: none">• 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 the topic about creating spaces for a site in the <i>ALM Octane Help Center</i>.
No	<p>Provide ALM Octane with a regular Oracle user with the following permissions for both site and space schemas. Both schemas must be created before installation.</p> <ul style="list-style-type: none">• CREATE TABLE• CREATE SESSION• CREATE SEQUENCE• The QUOTA clause on the user's default tablespace should be unlimited.

SQL Server database

These are the permissions user you will define for the user you will specify in the **DBAdminUser** setting in the **setup.xml** file. For details, see ["DBAdminUser" on page 28](#).

Permissions vary depending how you work with ALM Octane and how you want to install.

Do you want ALM Octane to create databases and login user during the installation?

Yes	<p>Use the sa user, or an ALM Octane database admin power user.</p> <p>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.</p> <p>Request that the SQL Server database admin create a temporary power user with the following privileges (roles), which are required to install ALM Octane:</p> <ul style="list-style-type: none">• Database Creators dbcreator role• Security Administrator securityadmin role <p>Note: It is important that the ALM Octane database administrative user is not the same as the ALM Octane admin user.</p> <p>The SQL Server database admin could name this power user octane_install_power_user, for example.</p> <p>For details on removing this temporary power user, see "Handle database-related issues" on page 78.</p>
No	<p>Create an ALM Octane database admin power user for installation purposes:</p> <ol style="list-style-type: none">1. Open the SQL Server Management Studio.2. In the Object Explorer pane, under the ALM Octane database server, expand the Security folder.3. Right-click the Logins folder, and select New Login.4. Type, for example, octane_install_power_user as the user name, and select the authentication type (enter the password if necessary).5. Click the Server Roles tab, and select the dbcreator and securityadmin options. Click OK.

Next steps:

- ["Deploy ALM Octane" on page 25](#)

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. For details, see ["Prerequisites" on page 15](#).
- Review security considerations in the knowledge base article [KM02707977](#).

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](#) 25
- [Configure initial site settings](#) 27
- [Configure other settings](#) 34
- [Update settings](#) 49
- [Initialize the ALM Octane server](#) 49

Deploy ALM Octane

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

In this topic:

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

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. For details, see ["Prerequisites" on page 15](#).
- Review security considerations in the knowledge base article [KM02707977](#).

Deploy

1. Download the ALM Octane package.

<https://software.microfocus.com/en-us/products/application-lifecycle-management/download>

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

setup.exe

Click **Next**.

3. In the setup dialog, set the following:

Installation folder	The folder in which to install ALM Octane. The default is C:\octane . Do not enter a name with spaces for the folder.
Service user	Whether the service should use the local system account or a specific user.
Service user domain	The domain of the user that will start the ALM Octane service. Available when the Service user is Specific user .

Service user name	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. Available when the Service user is Specific user .
Password	Password for the user that will start the ALM Octane service. Available when the Service user is Specific user .

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

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

Default folder	Description
C:\octane	ALM Octane installation folder and all its sub-directories and files. These files are used for configuring the server.
C:\octane\repo	The repository folder, and its site and spaces sub-directories. 2. Cluster configuration: <ul style="list-style-type: none"> • The repository folder has to be a shared folder visible to all cluster nodes. • It is important that you enter the repository path using the same path name on all nodes. For example, you cannot have the path on the first server node defined as C:\octane\repo and on additional nodes defined as C:\opt\octane\repo. • If the repository is not located on a remote, dedicated machine, the repository location cannot be C:\octane.
C:\octane\log	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

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.yml** file. For details, see ["Configure other settings" on page 34](#).
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.

Next steps:

- ["Configure initial site settings" on the next page](#)

Configure initial site settings

You can configure initial site settings using the **setup.xml** file. You must set the settings in the **setup.xml** file during the ALM Octane installation. These settings cannot be changed later.

In this topic:

- ["Configure initial site settings" above](#)
- ["Database server settings" below](#)
- ["Oracle server settings" on page 30](#)
- ["SQL Server settings" on page 30](#)
- ["Site actions" on page 30](#)
- ["Space settings" on page 31](#)
- ["Elasticsearch settings" on page 32](#)
- ["Site admin credential settings" on page 33](#)
- ["Repository settings" on page 33](#)
- ["Configure initial site settings" above](#)
- ["Additional settings" on page 34](#)

Overview

Configure these settings by editing the **setup.xml** file: `C:\octane\conf\setup.xml`

It is recommended that you save a local copy of the **setup.xml** file before making changes to it.

Also, for security purposes, **setup.xml** should be stored in a secure, off-site location.

Database server settings

The Oracle settings can be used for both Oracle and SQL server.

Oracle settings	Description
DBType	The supported database types are: <ul style="list-style-type: none">• ORACLE• MSSQL
SchemaName	The name of the site schema that is created by the DBAdminUser during the installation, or supplied by the organization's DBA. Enter the supplied name.

Oracle settings	Description
SchemaPassword	<p>For Oracle: The password of the site schema. Enter the supplied password.</p> <p>When using Oracle, and installing using existing site schemas (with the FILL_EXISTING site action), make sure that the passwords that the DBA defines for the site schema and the space schema both match this password.</p> <p>For SQL Server: The password for the DBLoginUser user.</p>
DBAdminUser	<p>ALM Octane uses this user both to create objects during installation and also to check that the database server is accessible.</p> <p>For Oracle:</p> <ul style="list-style-type: none"> • The name of the database admin user (DBAdminUser). • When using Oracle, and installing using existing site schemas (with the FILL_EXISTING site action), enter the SchemaName instead. <p>For SQL Server:</p> <p>Login object for logging into the database instance. ALM Octane uses this login for setup, tables, and indexes.</p> <ul style="list-style-type: none"> • This is either the sa user or an SQL Server power user with the correct permissions. • When using SQL Server, and installing using the FILL_EXISTING site action, enter the DBAdminUser setting. <p>For details about DBAdminUser permissions, see "Permissions" on page 22.</p> <p>For the FILL_EXISTING site action, make sure to also specify SharedSpaceSchemaName.</p>
DBAdminPassword	<p>For Oracle: The password of the database admin user (DBAdminUser).</p> <ul style="list-style-type: none"> • Do not include a pound sign (#) or accented characters (such as, ä, ç, ñ). • When installing using existing site schemas (with the FILL_EXISTING site action), enter the SchemaPassword instead. <p>For SQL Server: The Password for the sa user or the SQL Server power user defined with the DBAdminUser setting.</p> <ul style="list-style-type: none"> • When installing using existing site database instances (with the FILL_EXISTING site action), enter the SchemaPassword instead.

Oracle settings	Description
ConnectionString	<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> <p>The instructions below demonstrate how to set up the string with non-secured database access. However, you can use this connection string to configure secure access to the database.</p> <h3>Oracle</h3> <ul style="list-style-type: none">• Syntax using TNS alias names: To use TNS alias names, make sure to provide a value for the DBServerName setting. <pre><entry key="ConnectionString">jdbc:mercury:oracle:TNSNamesFile=/<path>/tnsnames.ora;TNSServerName=<server_name></entry></pre>Example: <pre>jdbc:mercury:oracle:TNSNamesFile=/etc/tnsnames.ora;TNSServerName=ora12</pre>• Syntax using service names: <pre><entry key="ConnectionString">jdbc:mercury:oracle://<DB_SERVER_NAME>:<DB_SERVER_PORT>;servicename=<DB_SERVICE_NAME></entry></pre>Example: <pre>jdbc:mercury:oracle://dbserver1.net:1521;servicename=orcl</pre><p>To connect to Oracle RAC, use the Single Client Access Name (SCAN) instead of the database server name.</p>• Syntax using port: <pre><entry key="ConnectionString">jdbc:mercury:sqlserver://DB_SERVER_NAME:DB_SERVER_PORT</entry></pre>Example: <pre>jdbc:mercury:sqlserver://dbserver1:1433</pre>• Syntax using instance: <pre><entry key="ConnectionString">jdbc:mercury:sqlserver://DB_SERVER_NAME/INSTANCE_NAME</entry></pre>Example: <pre>jdbc:mercury:sqlserver://dbserver1:my_instance</pre>

Oracle server settings

Oracle Settings	Description
TableSpace	The tablespace in the Oracle database where the site schema segment will be created. Case-sensitive.
TempTableSpace	The temporary tablespace in the Oracle database. Case-sensitive.
DBServerName	The TNS alias name for connecting to the Oracle database. Optional. For use with " Configure initial site settings " on page 27. Example: dbserver1.net
DBServerPort	The port for connecting to the Oracle database.

SQL Server settings

SQL Server settings	Description
	<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> <p>Specify the password for this user using the SchemaPassword setting. Do not include a pound sign (#) or accented characters (such as, ä, ç, ñ).</p> <p>If the DBLoginUser user already exists, make sure to use the existing user's password.</p>

Site actions

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

CREATE_NEW	<p>Use this site action for new installations.</p> <ul style="list-style-type: none">• Creates a new site schema, creates a new space schema, and configures the current node.• Only a DBAdminUser with create schema permissions can create a new schema.• The CREATE_NEW site action fails when the schema already exists.
-------------------	--

FILL_ EXISTING	<p>Use this site action for new installations, in cases where the database admin user 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 creates a new site and a new space schema/database, and users. See this SQL Server example.</p> <p>For SQL Server:</p> <p>Two databases are created, one for the site and one for the space . Both are created by the DBA.</p> <ul style="list-style-type: none">• The default collation is SQL_Latin1_General_CP1_CI_AS (must be case-insensitive).• Make sure you specify these databases in the SchemaName and SharedSpaceSchemaName settings, because they are mandatory.• Make sure you define the SchemaPassword setting. <p>For Oracle:</p> <p>Two schemas are created, one for the site and one for the space. Both are created by the DBA.</p> <p>SharedSpaceSchemaName should have the same password as SchemaName.</p> <p>Make sure that the passwords that the DBA defines for the site schema and the space schema both match the SchemaPassword setting.</p> <p>Handling schema/database exceptions</p> <p>If the organization's DBA made changes to schemas/databases, 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 "Using exception files for manual database changes" on page 81.</p> <p>For SQL Server: Example of creating a database and granting user access</p> <pre>CREATE DATABASE <database_name> CREATE LOGIN <login_name> WITH PASSWORD = 'thepassword', CHECK_POLICY = OFF USE <database_name> sp_adduser '<logName>' , 'octane' GRANT ALL TO octane sp_addrolemember 'db_ddladmin', 'octane'</pre>
---------------------------------	--

Space settings

Where relevant, the Oracle settings can be used for both Oracle and SQL server. Alternatively, for SQL Server, you can specify the SQL Server settings instead.

Oracle settings	SQL Server settings	Description
SharedSpaceSchemaName	MssqlSharedspaceDatabaseName	<p>Relevant only for the FILL_EXISTING site action.</p> <p>For Oracle:</p> <p>To configure the space, add a SharedSpaceSchemaName parameter and set it to the name of the schema that is designated for the space.</p> <p>For SQL Server:</p> <p>To configure the space, add a MssqlSharedspaceDatabaseName parameter and set it to the name of the database that is designated for the space.</p>
DefaultSpaceMode	<NA>	<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"> • isolated. Workspaces associated with the initial space will not share entities or customization settings. • shared. Workspaces associated with the initial space can share entities or customization settings. <p>Examples:</p> <pre><entry key="DefaultSpaceMode">isolated</entry> <entry key="DefaultSpaceMode">shared</entry></pre>

Elasticsearch settings

A working Elasticsearch server is a requirement for working with ALM Octane. Make sure you are using a version supported by ALM Octane:

- For the supported version, see the requirements for [Database and Elasticsearch](#).
- For details on installing Elasticsearch, see knowledge base article [KM02494295](#).
- For details on upgrading to a new Elasticsearch version, see knowledge base article [KM03207448](#).

ElasticHost	<p>The name of the host running Elasticsearch.</p> <p>If running an Elasticsearch cluster, all node host names should be separated by semi-colons (;).</p> <p>Example: host1;host2;host3</p>
ElasticPort	<p>The number of the port running the Elasticsearch binary service.</p> <p>This port must be accessible from the ALM Octane server, not just by checking the HTTP connection.</p> <p>Example: 9300</p>
ElasticClusterName	<p>The name of the Elasticsearch cluster.</p>

Site admin credential settings

SiteAdministratorUser	<p>The email of the site admin user that the installation will create.</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>
SiteAdministratorPassword	<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>

Repository settings

RepositoryFolder	<p>The full path of the repository folder.</p> <p>Example: C:\octane\repo</p> <p>Cluster configuration:</p> <ul style="list-style-type: none">• The folder specified here must be accessible to all cluster nodes.• If the repository is not located on a remote, dedicated machine, the repository location cannot be C:\octane.
-------------------------	---

Additional settings

AppURL	<p>The fully-qualified domain name and port for the ALM Octane server. This URL is 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://<Server URL>:[Port]</code></p> <p>Basic configuration: Usually the URL of the server on which you installed the ALM Octane server.</p> <p>Cluster configuration: The Virtual IP URL.</p>
---------------	---

Next steps:

- ["Configure other settings" below](#)

Configure other settings

You can configure additional site settings using the **octane.yml** file. These settings are configured during installation, and can also be changed any time, whenever necessary.

In this topic:

- ["Overview" below](#)
- ["Rules for editing the octane.yml file" below](#)
- ["General server settings" on the next page](#)
- ["LDAP settings" on page 36](#)
- ["License settings" on page 41](#)
- ["Oracle settings" on page 42](#)
- ["Cluster settings" on page 42](#)
- ["ALM Octane service provider \(SP\) settings" on page 43](#)

Overview


If you update any of these settings at a later time, make sure you restart the ALM Octane server. 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.

Configure these settings by editing the **octane.yml** using any editor: `C:\octane\conf\octane.yml`.

Rules for editing the octane.yml file



Caution: Correct indentation and formatting is essential when editing **yml** files to avoid

 unpredictable results during installation.

There are resources available online that describe the exact rules and conventions for formatting **yml** files. We strongly recommend that you familiarize yourself with these rules before editing **octane.yml**.


Here are some important rules when editing settings in **octane.yml**:

- Put a single space after the colon between the parameter name and the value.
- Do not add bullets or any other extra formatting.
- Do not add extra spaces.
- Use double quotes to enclose any values that include special characters, especially the **#**.
A **#** that is not enclosed in quotes marks the beginning of a comment. Any text after it, until the end of the line, is ignored. The **octane.yml** file is then interpreted incorrectly during installation and causes errors.

If these conventions are not followed, ALM Octane initialization or upgrade can fail.

For an example, see the sample **octaneExample.yml** file.

General server settings

cluster	<p>Cluster configuration: Enter a comma-separated list of node host names or IPs in the cluster.</p> <p> Example: 10.0.0.24,10.0.0.99,10.0.0.23</p> <p>This is a mandatory setting.</p> <p>By default, the cluster is not configured, and the default value is blank. This indicates a standalone ALM Octane server.</p>
heapSize	<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>heapSize should be set 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: 4096</p>

server	<p>The value of a Jetty port for HTTP, or a Jetty secure port for HTTPS.</p> <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> <p>httpPort: 8080</p> <p>httpsPort: 8443</p> <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>
proxy	<p>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.</p> <p>An example of accessing an external server is when using a Trigger webhook rule.</p> <p>host: <proxy_host></p> <p>port: <proxy_port></p> <p>user: <user></p> <p>password: <password></p>
authenticationType	<p>Whether the ALM Octane installation should use native user management or LDAP authentication for user management.</p> <p>Values are:</p> <p>sso. Use SSO authentication.</p> <p>ldap. Use LDAP authentication.</p> <p>internal. Use internal, native ALM Octane user management. Default.</p>

LDAP settings

If you are planning on authenticating users using LDAP, set the **authenticationType** setting is set to **ldap**, and define the following settings.

Later, after ALM Octane installation, import users from LDAP into ALM Octane. See the information about setting up LDAP user authentication in the *ALM Octane Help Center*.

Note: After updating the **octane.yml** file, 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.

Make sure your LDAP system has the corresponding attributes for each mandatory LDAP setting.

General LDAP settings

connectionTimeout	<p>Connection timeout in seconds. Optional.</p> <p>Default: 30 seconds</p>
adminDn	<p>The user that will log on to ALM Octane after initially 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 octane.yml, verifies that this user exists, and validates this user against the LDAP data. If this attribute is not defined correctly, the server will not start. Correct the user details and restart the server.</p> <p>This user can be same user as the user entered in the setup.xml 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 setup.xml file is overwritten.</p> <p>Note: If the adminDn is changed and the server is restarted, both the original adminDn and the new adminDn exist as site admins. Modifying the adminDn does not remove the original one.</p>

LDAP server settings

Make sure your LDAP system has the corresponding attributes for each mandatory LDAP setting.

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

Enter the following settings for each LDAP server separately.

Each LDAP server is defined by a group of settings. The settings for each LDAP server start with a hyphen (-) followed by the **host** setting.

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

servers	Header row to delineate that the information below is for each LDAP server. Do not enter a value.
host	<p>The LDAP server host name or IP address. Mandatory.</p> <p>Prefix each host item with a - sign: - host. This instructs ALM Octane where each host begins, especially if there are multiple LDAP servers.</p>
port	LDAP server connection port. Mandatory.

isSsl	<p>Whether the LDAP server uses SSL. Mandatory.</p> <p>Enter Y or N.</p> <p>If Y, establish trust to the certificate authority that issued the LDAP server certificate. For details, see Configure trust on the server.</p>
description	<p>Description of the LDAP server. Optional.</p>
baseDirectories	<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>If specified,</p> <p>Make sure to put a space after hyphen (-) before specifying the filter.</p> <p>Example:</p> <p>baseDirectories:</p> <ul style="list-style-type: none"> - ou=Groups,o=organization.com - dc=maxcrc,dc=com
baseFilters	<p>Filters to use to refine the search for users when including new LDAP users in ALM Octane spaces. This is generally a list of LDAP objectClasses.</p> <p>Optional. Default: (objectClass=*)</p> <p>Make sure to put a space after hyphen (-) before specifying the filter.</p> <p>Example:</p> <p>baseFilters:</p> <ul style="list-style-type: none"> - (objectClass=*) - (&(objectClass=user)(objectCategory=person))
authentication:	<p>Header row to delineate that the information below is for authentication. Do not enter a value.</p>
method	<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"> • anonymous. In this case, skip the next two parameters, user and password. • simple, user, and password are mandatory.
user	<p>Only required if you set the authentication parameter to simple.</p> <p>User name for accessing the LDAP server. This user must have at least read permissions for the LDAP server.</p>
password	<p>Only required if you set the authentication parameter to simple.</p> <p>Password for accessing the LDAP server.</p> <p>This password will be encrypted.</p>

LDAP server mapping settings

Make sure your LDAP system has the corresponding attributes for each mandatory LDAP setting.

Enter the following mapping settings for each LDAP server separately.

Values used in the mapping section are case-sensitive.

ALM Octane attribute in octane.yml	Sample LDAP attribute that can be used	Values and descriptions
mapping		Header row to delineate that the information below is for mapping of LDAP attributes. Do not enter a value.
dn	distinguishedName (for Active Directory)	<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>cn=<common_name>,ou=<organizational_unit>,dc=<part_of_domain></p> <p>The dn is a unique string that typically contains other LDAP attributes, such as cn, ou, and dc.</p>
	entryDN (for other LDAP systems)	<p>Example</p> <ol style="list-style-type: none"> 1. If in LDAP, the entryDN attribute value is: cn=<common_name>,ou=<organizational_unit>,dc=<part_of_domain> 2. In the octane.yml, the dn value would be mapped to: entryDN 3. When exporting users from LDAP, the dn 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: cn=Joe_Smith@nga,ou=my_org,dc=com

ALM Octane attribute in octane.yml	Sample LDAP attribute that can be used	Values and descriptions
uid	objectGUID (for Active Directory)	<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> <p>To work with ALM Octane with Active Directory, we use objectGUID.</p> <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>
	entryUUID (for other LDAP systems)	<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> <p>To work with ALM Octane, we generally use entryUUID for OpenLDAP. However, depending on your LDAP, this attribute might be different, such as GUID or orclguid.</p> <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>
	You can configure other values, such as GUID or orclguid, or any other unique value.	
firstName	givenName	LDAP attribute for first name, such as givenName . Mandatory.
lastName	sn	LDAP attribute for last name, such as sn . Mandatory.
fullName	cn	LDAP attribute for full name, such as cn . Optional.
logonName	mail	<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>mail is usually unique for each user, so mail is an appropriate LDAP attribute to use to map to logonName. Mandatory.</p> <p>You can change the logonName attribute mapping at any time, but make sure the logonName is unique across all ALM Octane users.</p>
email	mail	The LDAP attribute for email address, such as mail . Mandatory.
phone1	telephoneNumber	The LDAP attribute for the primary phone number, such as telephoneNumber . Optional.

License settings

Locate the section called **license**, and enter values for the following settings.



Caution: If you plan to install a license for Team Edition at a later stage, you must enter **team** in the **trialEdition** field now.

Installing a license for Team Edition after an Enterprise Edition trial is not supported.

trialEdition	Enter team or enterprise , depending on your trial edition. For details, see the information about ALM Octane editions in the <i>ALM Octane User Guide</i> . Note: This setting is used the first time the ALM Octane server starts, and cannot be changed retroactively.
mode	<ul style="list-style-type: none">• If you are using a standalone ALM Octane license, enter standalone. You can then skip the remaining fields in the License section. Default.• If you are allocating licenses from ALM to ALM Octane, enter almSharing. You then need to fill in the following fields as described below.
The following fields are mandatory for almSharing mode:	
url	Enter the full path that you use to access ALM. Typically, this includes the suffix qcbn .
almIntegrationUser	Enter the user name for accessing ALM. This user was defined in ALM for integration purposes.
almIntegrationPassword	Enter the password for the almIntegrationUser . This password is automatically encrypted after you restart the ALM Octane server.

Oracle settings

The following Oracle section and its settings are also available.

Section	Setting	Description and usage
oracle_database:	useDefaultSort	<p>For Oracle databases: Defines whether the standard Oracle binary sort (NLS_SORT="BINARY_CI") should be overridden for non-Latin language support.</p> <p>Valid values: yes, no, or blank</p> <p>Default: blank (yes)</p> <p>Usage:</p> <pre>oracle_database: useDefaultSort: no</pre>

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 \(optional\)" on page 50](#).

cluster:	<p>Section header. Do not edit.</p> <pre>cluster: isCluster: true nodes:</pre>
<p>isCluster</p> <p>Available with 12.60 CP8 and later.</p>	<p>Whether your server is standalone or in a cluster configuration.</p> <p>Mandatory.</p> <p>For a cluster configuration, set this value to true. You must enter node host names in the nodes setting.</p> <p>For a standalone server, set this value to false and do not enter any host names using the nodes setting.</p> <p>Default: true</p>

nodes:	<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.</p> <p>Examples:</p> <ul style="list-style-type: none">• server1.domain.com,server2.domain.com,server3.domain.com• 120.150.12.12,120.150.80.13,120.150.32.14 <p>Make sure isCluster is set to true.</p>
---------------	--

ALM Octane service provider (SP) settings

The following service provider (SP) section and its settings are also available. Use these settings to set up SSO authentication for connecting to ALM Octane.

For these settings to take affect, make sure to set the authentication type to **sso** in this **octane.yml** file using the **authenticationType** setting.

For an example of setting these parameters, see the **octaneExample.yml** file.

Main settings

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

Setting	Description and usage
sso.keystore.file	<p>The absolute path to the keystore file identified with sso.key-pair.alias.</p> <p>The default format for this file is PKCS12. You can change the format to Java KeyStore (JKS) by specifying this type when adding the sso.oauth-keystore.type setting to octane.yml.</p> <p>The path should be under ALM Octane's configuration folder to avoid permission issues.</p> <p>Mandatory.</p>
sso.keystore.pwd	<p>Password used to protect the keystore file defined with sso.keystore.file.</p> <p>When ALM Octane starts, it encrypts this password.</p> <p>Mandatory.</p> <p>Example: my-password</p>
sso.login.saml2.idp.metadata-url	<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 sso.login.saml2.idp.metadata setting.</p> <p>Mandatory, if sso.login.saml2.idp.metadata is not defined.</p> <p>Example: http://my-server.company-infra.net:8080/auth/realms/Dev/protocol/saml/descriptor</p>

Setting	Description and usage
<p>sso.login.saml2.idp.metadata</p>	<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. If metadata is provided using this setting, the URL defined in sso.saml2.idp.metadata-url is ignored.</p> <p>Mandatory, if sso.login.saml2.idp.metadata-url is not defined.</p> <p>You can define the SAML metadata descriptor resource with either this setting or the sso.login.saml2.idp.metadata-url setting.</p>
<p>sso.oauth.authentication.timeout.seconds</p>	<p>The SSO authentication timeout in seconds.</p> <p>Optional.</p> <p>Default: 10800 seconds (3 hours).</p> <p>Other timeout settings when working with SSO</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 octane.yml file. They do not have any affect on the SSO authentication timeout.</p> <ul style="list-style-type: none"> • MINUTES_UNTIL_IDLE_SESSION_TIMEOUT. Defines license consumption in minutes. • MINUTES_UNTIL_GLOBAL_SESSION_TIMEOUT. Defines API key authorization timeout in minutes. <p>For details on setting these configuration parameters, see Configuration parameters.</p>
<p>sso.oauth.client.id</p>	<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: my-client-ID</p>

Setting	Description and usage
sso.oauth.client.secret	<p>The OAuth client secret for the integration's client ID defined with sso.oauth.client.id.</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: secret</p>
sso.saml.mapping.username	<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"> • {Sid}: Mapping is to the NameID in the SAML response's subject. Default. • userName: Mapping is to the username in the SAML attribute statement. <p>Changing the default to a property name, such as userName, in the SAML response, does not require quotes.</p>

Additional settings

Setting	Description and usage
sso.logging.console.enabled	<p>Whether to log to the console. Log messages are issued to the ALM Octane wrapper.log file.</p> <p>Optional.</p> <p>Default: false</p>
sso.logging.file.dir	<p>The directory in which to create the SSO log files.</p> <p>Optional.</p> <p>Default: <log folder>/sso</p>

Setting	Description and usage
sso.logging.file.enabled	<p>Whether to log to the ALM Octane file in the directory defined by the sso.logging.file.dir attribute.</p> <p>Optional.</p> <p>Default: true</p>
sso.logging.level	<p>Logging level. Possible values are:</p> <ul style="list-style-type: none">• SEVERE• INFO• WARNING• ALL <p>Optional.</p> <p>Default: WARNING</p>
sso.login.saml2.subject.format	<p>The format of the NameIDPolicy attribute in the SAML request.</p> <p>Default: urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</p>
sso.oauth.client.redirect-uri.host	<p>The domain name used to redirect back to ALM Octane. Regular expressions are supported, for example, .*mydomain.*</p> <p>Optional.</p> <p>in the domain from the AppURL setting as defined in the setup.xml file, surrounded by wildcards.</p> <p>Example: .*company-infra.net.*</p> <p>Caution: The redirect URI is a critical part of the OAuth flow. After a user successfully authorizes an application, the authorization server redirects the user back to the application with the authorization code in the URL. Because the redirect URL contains sensitive information, it is critical that the service does not redirect the user to arbitrary locations.</p>

Setting	Description and usage
sso.oauth.client.redirect-uri.schema	<p>The schema (http or https) used to access ALM Octane.</p> <p>Optional.</p> <p>Default: The schema in the AppURL setting defined in the setup.xml file.</p> <p>Caution: The redirect URI is a critical part of the OAuth flow. After a user successfully authorizes an application, the authorization server redirects the user back to the application with the authorization code in the URL. Because the redirect URL contains sensitive information, it is critical that the service does not redirect the user to arbitrary locations.</p>
sso.saml.mapping.firstName	<p>The attribute in the SAML response's attribute statement that maps to the user's first name.</p> <p>Optional.</p> <p>Default: firstName</p>
sso.saml.mapping.fullName	<p>The attribute in the SAML response's attribute statement that maps to the user's full name.</p> <p>Optional.</p> <p>Default: fullName</p>
sso.saml.mapping.lastName	<p>The attribute in the SAML response's attribute statement that maps to the user's last name.</p> <p>Optional.</p> <p>Default: lastName</p>
sso.saml.mapping.mail	<p>The attribute in the SAML response's attribute statement that maps to the user's email address.</p> <p>Optional.</p> <p>Default: mail</p>
sso.saml.mapping.uuid	<p>The attribute in the SAML response's attribute statement that maps to the user's UUID.</p> <p>Optional.</p> <p>Default: uuid</p>



Next steps:

- ["Update settings" below](#)

Update settings

If you have previously installed ALM Octane before, update the configuration settings.

If you have never installed ALM Octane on this machine, skip to ["Initialize the ALM Octane server" below](#).

How to update settings

1. Select **Start > ALM Octane > Update ALM Octane Settings**.

Alternatively, open a command prompt and run:

```
C:\octane\install\updatesettings.bat
```

Next steps:

- ["Initialize the ALM Octane server" below](#)

Initialize the ALM Octane server

You are now ready to initialize the ALM Octane server by starting the ALM Octane service.

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

Alternatively, run **initserver.bat**:

```
C:\octane\install\initserver.bat
```

The initialization keeps track of the last successful step that it performed; If for some reason you have to rerun **initserver.bat**, it only starts at the relevant point.

The ALM Octane service is now running. You can check Microsoft Windows **Services** to verify.

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

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 \(optional\)" on the next page](#).

Next steps:

- ["Log in to ALM Octane" below](#)
- ["Cluster installation \(optional\)" below](#)

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 the topic about trial licenses in the *ALM Octane Help Center*.

1. In a browser, navigate 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 **setup.xml** file using settings **SiteAdministratorUser** and **SiteAdministratorPassword**.

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. For details, see [Troubleshooting](#).

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 \(optional\)" below](#).
- Set configuration parameters, such as FORGET_USER_ON_DELETE and SMTP_NOTIFICATION_SENDER_EMAIL. See the topic about configuration parameters in the *ALM Octane Help Center*.
- Create spaces. See the topic about creating spaces in the *ALM Octane Help Center*.
- Once you have logged on as the space admin, you can create other users and workspaces. See the topics on ways to add users and how to create workspaces in the *ALM Octane Help Center*.

Cluster installation (optional)

This section provides end-to-end instructions for installing an on-premises ALM Octane server in a cluster configuration on Windows.

In this topic:

- ["Overview" on the next page](#)
- ["Install ALM Octane in a cluster configuration" on page 52](#)

Overview

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."

We install ALM Octane in a cluster configuration by:

1. Verifying all requirements and prerequisites for every node in the configuration.
2. After you configured the **setup.xml** and **octane.yml** configuration files in the first node, copy these file to all other cluster nodes.
3. Start ALM Octane on all servers.

See also ["Installation flow" on page 13](#).

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 System requirements and " Prerequisites " on page 15 .
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	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. Generally, the repository is located on an NFS or SAN server. If the repository is not located on a remote, dedicated machine, the repository location cannot be C:\opt\octane . The repository must be configured to use the same mount point (path) on all nodes. It is important that you enter the repository path using the same path name on all nodes. For example, you cannot have the path on the first server node defined as C:\octane\repo and on additional nodes defined as C:\server1\octane\repo .
Check access between nodes	All nodes must have access to each other. Verify ports are open in your firewall. 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.. By default, outbound ports are open. Check inbound ports. For details, see Inbound and outbound communication for clusters .

2. Install ALM Octane on the first cluster node

Install ALM Octane on the first cluster node, as described under "[Installation](#)" on [page 23](#).

a. "[Deploy ALM Octane](#)" on [page 25](#)

Here we deploy the ALM Octane installation files onto the first node.

b. "[Configure initial site settings](#)" on [page 27](#)

We configure ALM Octane by modifying the **setup.xml** configuration file.

Make sure to set the following settings to values that all cluster nodes can access.

DBServerName	The database server on which the site database schema resides. For cluster environments only.
---------------------	--

RepositoryFolder	The shared repository that all cluster nodes can access (read and write).
-------------------------	---

c. ["Configure other settings" on page 34](#)

We configure other ALM Octane cluster settings by modifying the **octane.yml** configuration file.

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

cluster:	Section header. Do not edit. cluster: isCluster: true nodes:
isCluster Available with 12.60 CP8 and later.	Whether your server is standalone or in a cluster configuration. Mandatory. For a cluster configuration, set this value to true . You must enter node host names in the nodes setting. For a standalone server, set this value to false and do not enter any host names using the nodes setting. Default: true
nodes:	Configure the IP addresses or fully qualified domain names for each cluster node. Enter a comma-separated list of node host names, or IPs, in the cluster. Examples: ◦ server1.domain.com,server2.domain.com,server3.domain.com ◦ 120.150.12.12,120.150.80.13,120.150.32.14 Make sure isCluster is set to true .

d. ["Initialize the ALM Octane server" on page 49](#)

On the first node only, we initialize by running **initserver.bat**.



Caution: Never run **initserver.bat** on any other cluster nodes.

3. **Set up a secure configuration on the first cluster node**

If you want to set up a secure configuration for ALM Octane, follow the instructions in knowledge base article [KM02707977](#).

4. **Make sure ALM Octane is running on the first node in the cluster**

Before installing on remaining cluster nodes, log in to ALM Octane.

For details, see ["Log in to ALM Octane" on page 50](#).

5. **Only after you successfully log in, deploy ALM Octane installation files on each additional cluster node**

Download and deploy the ALM Octane package on each cluster node. For details, see ["Deploy ALM Octane" on page 25](#) and ["Deploy in cluster environment" on page 26](#).



Caution: Do not do the following:

- Do not configure the **setup.xml** and **octane.yml** files. You will be copying these files from the first node in the cluster during the next step.

6. **Configure each additional cluster node**

Copy the **C:\octane\conf\setup.xml** and **C:\octane\conf\octane.yml** files from the first cluster node to the **C:\octane\conf** folder on the cluster node.

7. **Start ALM Octane on each additional cluster node**

Select **Start > ALM Octane > Initialize ALM Octane Server** on each cluster node.

8. **Set up a secure configuration on each additional cluster node**

If you want to set up a secure configuration for ALM Octane in a cluster configuration, follow these instructions on each additional cluster node: [Software Self-solve knowledge base article KM02707977](#).

9. **Make sure ALM Octane is running on each additional node in the cluster**

For details, see ["Log in to ALM Octane" on page 50](#). Use the load balancer URL when you log in.

Upgrade

This section describes how to upgrade an existing installation of an on-premises ALM Octane server on Windows.

In this topic:

- ["Before you upgrade" on the next page](#)
- ["Deploy" on page 57](#)
- ["Configure initial settings" on page 57](#)
- ["Configure other settings" on page 58](#)
- ["Upgrade" on page 72](#)
- ["Configure and upgrade cluster nodes" on page 72](#)
- ["Upgrade spaces in ALM Octane" on page 73](#)
- ["Restart all Jetty servers" on page 73](#)
- ["After the upgrade" on page 74](#)
- ["Bulk update data access control" on page 74](#)

Before you upgrade

1. Verify that your server machine, and if relevant, all cluster nodes, meet all prerequisites.
This includes checking the supported versions for all third party tools, such as Elasticsearch, and upgrading accordingly.
For details, see ["Prerequisites" on page 15](#).

Note: If the following are both true, add the CREATE SEQUENCE privilege to the site and shared space schemas:

- You are upgrading from an ALM Octane version earlier than 12.55.3.
- You are upgrading an installation without a DB admin, for example, your original ALM Octane was installed using the FILL_EXISTING site action.

2. Create backups of:
 - The repository
 - Existing ALM Octane configuration files, including **setup.xml** and **octane.yml**
 - Your database
 - Elasticsearch
 - If you are using ALM Octane Synchronizer, back up :
 - **C:\octane\wrapper\wrapper.conf**
 - **Service.locator.properties.example (C:\octane\webapps)**

For recommendations on making these backups, see ["Best practices: Backing up ALM Octane data" on page 86](#).

3. Take note of any special aspects of your configuration, such as:

Special configuration	Recommendation
Did you install ALM Octane to a location other than C:\octane ?	Refer to the location you used while upgrading.
Did you modify the C:\opt\octane\webapps\root\WEB-INF\classes\hpssoconfig.xml file to control session timeouts?	If you modified the this file to control session timeouts, your updates will be overwritten by the upgrade. After upgrading, control session timeouts by setting the MINUTES_UNTIL_GLOBAL_SESSION_TIMEOUT and MINUTES_UNTIL_IDLE_SESSION_TIMEOUT configuration parameters instead. For details, see the topic about configuration parameters in the <i>ALM Octane Help Center</i> .
Do you want to switch from native user management to LDAP user management with this upgrade?	If you are upgrading from an ALM Octane version using native user management, and want to start using LDAP user management with this new ALM Octane version: <ul style="list-style-type: none"> a. Realize that once you configure for LDAP user management, you cannot return back to native, internal user management. b. When configuring initial settings in the setup.xml file, set the DefaultSpaceMode to isolated. For details, see "DefaultSpaceMode" on page 32. c. Upgrade ALM Octane without configuring for LDAP. This means, when modifying the octane.yml file, do not enter any values in the LDAP Settings section. d. After the upgrade is complete, configure for LDAP. e. Deactivate any native, internal users after LDAP configuration. These users can no longer log into ALM Octane (except for the adminDN user).
Did your organization's DBA made changes to database schemas, such as the addition of tables or columns?	Define an exception file. The exception file instructs ALM Octane to ignore manual changes to the database schemas during installation. For details, see "Using exception files for manual database changes" on page 81 .

4. Stop the ALM Octane service on the server, and if relevant, all cluster nodes.

Deploy

Download and deploy the new version of ALM Octane using:

```
setup.exe
```

For details, see ["Deploy ALM Octane" on page 25](#).

Configure initial settings

Here we describe how to modify settings in the **setup.xml** file.

1. Manually add newly-introduced settings to **setup.xml**

With each version of ALM Octane, settings are added to support new features. To upgrade to the new version, add the newly-introduced settings as listed in the table below to the **setup.xml** file.

Give these new settings values.

Here is a list of introduced settings for **setup.xml** by version:

Version	New Setting	Example
Introduced in 12.55.4, but mandatory as of 12.55.17	DefaultSpaceMode	<entry key="DefaultSpaceMode">shared</entry>
12.60.4	A new section, oracle_database , was added. It contains the new useDefaultSort setting.	See Oracle settings below.

- a. If not already open, open **C:\octane\conf\setup.xml** using an editor.
- b. Add any missing settings using this format:

```
<entry key="<setting>"><setting value></entry>
```

Do not modify any text in the <entry> and </entry> tags themselves. Only modify text between these tags.

- c. Save the file.

For a full list of settings for the current ALM Octane installation and their syntax, see ["Configure initial site settings" on page 27](#).

Configure other settings

Here we describe how to modify settings in the **octane.yml** file.

1. Learn the format for **yml** files

<setting> : <setting value>



Caution: Correct indentation and formatting is essential when editing **yml** files to avoid unpredictable results during installation.

There are resources available online that describe the exact rules and conventions for formatting **yml** files. We strongly recommend that you familiarize yourself with these rules before editing **octane.yml**.

Here are some important rules when editing settings in **octane.yml**:

- Put a single space after the colon between the parameter name and the value.
- Do not add bullets or any other extra formatting.
- Do not add extra spaces.
- Use double quotes to enclose any values that include special characters, especially the **#**.

A **#** that is not enclosed in quotes marks the beginning of a comment. Any text after it, until the end of the line, is ignored. The **octane.yml** file is then interpreted incorrectly during installation and causes errors.

If these conventions are not followed, ALM Octane initialization or upgrade can fail.

For an example, see the sample **octaneExample.yml** file.

2. Determine settings to add to, and remove from, **octane.yml**

With each version of ALM Octane, settings are added to support new features. To upgrade to the new version, add the newly-introduced settings as listed in the table below to the **octane.yml** file.

Version	Added / Removed	Example
12.55.4	In the LDAP settings section, added the following LDAP settings: dn uid baseDirectories baseFilters	<p>dn and uid example:</p> <pre>mapping: dn: entryDN uid: entryUUID</pre> <p>method example:</p> <pre>authentication: method: anonymous</pre> <p>baseDirectories example:</p> <pre>baseDirectories: - ou=Groups,o=organization.com - dc=maxcrc,dc=com</pre> <p>baseFilters example</p> <pre>baseFilters: - (objectClass=*) - (&(objectClass=user)(objectCategory=person))</pre>
12.55.17	In the License settings section, added the trialEdition setting.	See licenses below.
12.60.16	For support for SSO in federated environments, added the service provider section. Also added a new authentication type setting for SSO.	See SP Settings below. authenticationType: sso


3. Modify settings

- a. Edit the **C:\octane\conf\octane.yml** file using an editor.
- b. Locate the section for each setting you need to add.

- c. Add any missing settings as listed above using this format:

<setting> : <setting value>

General server settings

<p>cluster</p>	<p>Cluster configuration: Enter a comma-separated list of node host names or IPs in the cluster.</p> <div style="border: 1px solid purple; background-color: #f0f0f0; padding: 5px; margin: 10px 0;">  Example: 10.0.0.24,10.0.0.99,10.0.0.23 </div> <p>This is a mandatory setting.</p> <p>By default, the cluster is not configured, and the default value is blank. This indicates a standalone ALM Octane server.</p>
<p>heapSize</p>	<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>heapSize should be set 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: 4096</p>
<p>server</p>	<p>The value of a Jetty port for HTTP, or a Jetty secure port for HTTPS.</p> <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> <p>httpPort: 8080</p> <p>httpsPort: 8443</p> <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>

proxy	<p>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.</p> <p>An example of accessing an external server is when using a Trigger webhook rule.</p> <p>host: <i><proxy_host></i></p> <p>port: <i><proxy_port></i></p> <p>user: <i><user></i></p> <p>password: <i><password></i></p>
authenticationType	<p>Whether the ALM Octane installation should use native user management or LDAP authentication for user management.</p> <p>Values are:</p> <p>sso. Use SSO authentication.</p> <p>ldap. Use LDAP authentication.</p> <p>internal. Use internal, native ALM Octane user management. Default.</p>

LDAP settings

Make sure your LDAP system has the corresponding attributes for each mandatory LDAP setting.

connectionTimeout	<p>Connection timeout in seconds. Optional.</p> <p>Default: 30 seconds</p>
adminDn	<p>The user that will log on to ALM Octane after initially 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 octane.yml, verifies that this user exists, and validates this user against the LDAP data. If this attribute is not defined correctly, the server will not start. Correct the user details and restart the server.</p> <p>This user can be same user as the user entered in the setup.xml 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 setup.xml file is overwritten.</p> <p>Note: If the adminDn is changed and the server is restarted, both the original adminDn and the new adminDn exist as site admins. Modifying the adminDn does not remove the original one.</p>

LDAP server settings

Make sure your LDAP system has the corresponding attributes for each mandatory LDAP setting.

Enter the following settings for each LDAP server separately.

Each LDAP server is defined by a group of settings. The settings for each LDAP server start with a hyphen (-) followed by the **host** setting.

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

servers	Header row to delineate that the information below is for each LDAP server. Do not enter a value.
host	The LDAP server host name or IP address. Mandatory. Prefix each host item with a - sign: - host . This instructs ALM Octane where each host begins, especially if there are multiple LDAP servers.
port	LDAP server connection port. Mandatory.
isSsl	Whether the LDAP server uses SSL. Mandatory. Enter Y or N . If Y , establish trust to the certificate authority that issued the LDAP server certificate. For details, see Configure trust on the server .
description	Description of the LDAP server. Optional.
baseDirectories	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. Optional. Default: Blank. If specified, Make sure to put a space after hyphen (-) before specifying the filter. Example: baseDirectories: <ul style="list-style-type: none"> - ou=Groups,o=organization.com - dc=maxcrc,dc=com
baseFilters	Filters to use to refine the search for users when including new LDAP users in ALM Octane spaces. This is generally a list of LDAP objectClasses . Optional. Default: (objectClass=*) Make sure to put a space after hyphen (-) before specifying the filter. Example: baseFilters: <ul style="list-style-type: none"> - (objectClass=*) - (&(objectClass=user)(objectCategory=person))
authentication:	Header row to delineate that the information below is for authentication. Do not enter a value.

method	The LDAP authentication method supported by the LDAP server. Authentication method used by the LDAP server. The following methods are supported: <ul style="list-style-type: none"> o anonymous. In this case, skip the next two parameters, user and password. o simple, user, and password are mandatory.
user	Only required if you set the authentication parameter to simple . User name for accessing the LDAP server. This user must have at least read permissions for the LDAP server.
password	Only required if you set the authentication parameter to simple . Password for accessing the LDAP server. This password will be encrypted.

LDAP server mapping settings

Make sure your LDAP system has the corresponding attributes for each mandatory LDAP setting.

Enter the following mapping settings for each LDAP server separately.

Values used in the mapping section are case-sensitive.

ALM Octane attribute in octane.yml	Sample LDAP attribute that can be used	Values and descriptions
mapping		Header row to delineate that the information below is for mapping of LDAP attributes. Do not enter a value.

ALM Octane attribute in octane.yml	Sample LDAP attribute that can be used	Values and descriptions
dn	distinguishedName (for Active Directory)	<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>cn=<common_name>,ou=<organizational_unit>,dc=<part_of_domain></p> <p>The dn is a unique string that typically contains other LDAP attributes, such as cn, ou, and dc.</p>
	entryDN (for other LDAP systems)	<p>Example</p> <ul style="list-style-type: none"> i. If in LDAP, the entryDN attribute value is: cn=<common_name>,ou=<organizational_unit>,dc=<part_of_domain> ii. In the octane.yml, the dn value would be mapped to: entryDN iii. When exporting users from LDAP, the dn 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: cn=Joe_Smith@nga,ou=my_org,dc=com

ALM Octane attribute in octane.yml	Sample LDAP attribute that can be used	Values and descriptions
uid	objectGUID (for Active Directory)	<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> <p>To work with ALM Octane with Active Directory, we use objectGUID.</p> <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>
	entryUUID (for other LDAP systems)	<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> <p>To work with ALM Octane, we generally use entryUUID for OpenLDAP. However, depending on your LDAP, this attribute might be different, such as GUID or orclguid.</p> <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>
	You can configure other values, such as GUID or orclguid, or any other unique value.	
firstName	givenName	LDAP attribute for first name, such as givenName . Mandatory.
lastName	sn	LDAP attribute for last name, such as sn . Mandatory.
fullName	cn	LDAP attribute for full name, such as cn . Optional.
logonName	mail	<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>mail is usually unique for each user, so mail is an appropriate LDAP attribute to use to map to logonName. Mandatory.</p> <p>d. You can change the logonName attribute mapping at any time, but make sure the logonName is unique across all ALM Octane users.</p>
email	mail	The LDAP attribute for email address, such as mail . Mandatory.

ALM Octane attribute in octane.yml	Sample LDAP attribute that can be used	Values and descriptions
phone1	telephoneNumber	The LDAP attribute for the primary phone number, such as telephoneNumber . Optional.

License settings

trialEdition	<p>Enter team or enterprise, depending on your trial edition. For details, see the information about ALM Octane editions in the <i>ALM Octane User Guide</i>.</p> <div style="border-left: 2px solid green; padding-left: 10px; margin-top: 10px;"> <p>Note: This setting is used the first time the ALM Octane server starts, and cannot be changed retroactively.</p> </div>
mode	<ul style="list-style-type: none"> ○ If you are using a standalone ALM Octane license, enter standalone. You can then skip the remaining fields in the License section. Default. ○ If you are allocating licenses from ALM to ALM Octane, enter almSharing. You then need to fill in the following fields as described below.
The following fields are mandatory for almSharing mode:	
url	Enter the full path that you use to access ALM. Typically, this includes the suffix qcbn .
almIntegrationUser	Enter the user name for accessing ALM. This user was defined in ALM for integration purposes.
almIntegrationPassword	<p>Enter the password for the almIntegrationUser.</p> <p>This password is automatically encrypted after you restart the ALM Octane server.</p>

Oracle settings

Section	Setting	Description and usage
oracle_database:	useDefaultSort	<p>For Oracle databases: Defines whether the standard Oracle binary sort (NLS_SORT="BINARY_CI") should be overridden for non-Latin language support.</p> <p>Valid values: yes, no, or blank</p> <p>Default: blank (yes)</p> <p>Usage:</p> <pre>oracle_database: useDefaultSort: no</pre>

ALM Octane service provider (SP) settings

The following service provider (SP) section and its settings are also available. Use these settings to set up SSO authentication for connecting to ALM Octane.

For these settings to take affect, make sure to set the authentication type to **sso** in this **octane.yml** file using the **authenticationType** setting.

For an example of setting these parameters, see the **octaneExample.yml** file.

Main settings

Setting	Description and usage
sso.key-pair.alias	Unique identifier for the SSO public/private key pair used by the ALM Octane service provider for signing and encrypting authentication information. Mandatory. Example: sso-osp-keypair
sso.key-pair.pwd	Password for protecting and encrypting the key pair defined with sso.key-pair.alias . When ALM Octane starts, it encrypts this password. Mandatory. Example: my-secret
sso.keystore.file	The absolute path to the keystore file identified with sso.key-pair.alias . The default format for this file is PKCS12 . You can change the format to Java KeyStore (JKS) by specifying this type when adding the sso.oauth-keystore.type setting to octane.yml . The path should be under ALM Octane's configuration folder to avoid permission issues. Mandatory.
sso.keystore.pwd	Password used to protect the keystore file defined with sso.keystore.file . When ALM Octane starts, it encrypts this password. Mandatory. Example: my-password

Setting	Description and usage
sso.login.saml2.idp.metadata-url	<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 sso.login.saml2.idp.metadata setting.</p> <p>Mandatory, if sso.login.saml2.idp.metadata is not defined.</p> <p>Example: http://my-server.company-infra.net:8080/auth/realms/Dev/protocol/saml/descriptor</p>
sso.login.saml2.idp.metadata	<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. If metadata is provided using this setting, the URL defined in sso.saml2.idp.metadata-url is ignored.</p> <p>Mandatory, if sso.login.saml2.idp.metadata-url is not defined.</p> <p>You can define the SAML metadata descriptor resource with either this setting or the sso.login.saml2.idp.metadata-url setting.</p>

Setting	Description and usage
sso.oauth.authentication.timeout.seconds	<p>The SSO authentication timeout in seconds.</p> <p>Optional.</p> <p>Default: 10800 seconds (3 hours).</p> <p>Other timeout settings when working with SSO</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 octane.yml file. They do not have any affect on the SSO authentication timeout.</p> <ul style="list-style-type: none">◦ MINUTES_UNTIL_IDLE_SESSION_TIMEOUT. Defines license consumption in minutes.◦ MINUTES_UNTIL_GLOBAL_SESSION_TIMEOUT. Defines API key authorization timeout in minutes. <p>For details on setting these configuration parameters, see Configuration parameters.</p>
sso.oauth.client.id	<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: my-client-ID</p>
sso.oauth.client.secret	<p>The OAuth client secret for the integration's client ID defined with sso.oauth.client.id.</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: secret</p>

Setting	Description and usage
sso.saml.mapping.username	<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"> ◦ '\${id}'. Mapping is to the NameID in the SAML response's subject. Default. ◦ userName. Mapping is to the username in the SAML attribute statement. <p>Changing the default to a property name, such as userName, in the SAML response, does not require quotes.</p>

Additional settings

Setting	Description and usage
sso.logging.console.enabled	<p>Whether to log to the console. Log messages are issued to the ALM Octane wrapper.log file.</p> <p>Optional.</p> <p>Default: false</p>
sso.logging.file.dir	<p>The directory in which to create the SSO log files.</p> <p>Optional.</p> <p>Default: <log folder>/sso</p>
sso.logging.file.enabled	<p>Whether to log to the ALM Octane file in the directory defined by the sso.logging.file.dir attribute.</p> <p>Optional.</p> <p>Default: true</p>
sso.logging.level	<p>Logging level. Possible values are:</p> <ul style="list-style-type: none"> ◦ SEVERE ◦ INFO ◦ WARNING ◦ ALL <p>Optional.</p> <p>Default: WARNING</p>

Setting	Description and usage
sso.login.saml2.subject.format	<p>The format of the NameIDPolicy attribute in the SAML request.</p> <p>Default: urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</p>
sso.oauth.client.redirect-uri.host	<p>The domain name used to redirect back to ALM Octane. Regular expressions are supported, for example, .*mydomain.*</p> <p>Optional.</p> <p>in the domain from the AppURL setting as defined in the setup.xml file, surrounded by wildcards.</p> <p>Example: .*company-infra.net.*</p> <p>Caution: The redirect URI is a critical part of the OAuth flow. After a user successfully authorizes an application, the authorization server redirects the user back to the application with the authorization code in the URL. Because the redirect URL contains sensitive information, it is critical that the service does not redirect the user to arbitrary locations.</p>
sso.oauth.client.redirect-uri.schema	<p>The schema (http or https) used to access ALM Octane.</p> <p>Optional.</p> <p>Default: The schema in the AppURL setting defined in the setup.xml file.</p> <p>Caution: The redirect URI is a critical part of the OAuth flow. After a user successfully authorizes an application, the authorization server redirects the user back to the application with the authorization code in the URL. Because the redirect URL contains sensitive information, it is critical that the service does not redirect the user to arbitrary locations.</p>
sso.saml.mapping.firstName	<p>The attribute in the SAML response's attribute statement that maps to the user's first name.</p> <p>Optional.</p> <p>Default: firstName</p>

Setting	Description and usage
sso.saml.mapping.fullName	The attribute in the SAML response's attribute statement that maps to the user's full name. Optional. Default: fullName
sso.saml.mapping.lastName	The attribute in the SAML response's attribute statement that maps to the user's last name. Optional. Default: lastName
sso.saml.mapping.mail	The attribute in the SAML response's attribute statement that maps to the user's email address. Optional. Default: mail
sso.saml.mapping.uuid	The attribute in the SAML response's attribute statement that maps to the user's UUID. Optional. Default: uuid

- d. Save the file.


Upgrade

1. On the server machine, select **Start > ALM Octane > Initialize ALM Octane Server**.


Alternatively, run **initserver.bat**:

```
C:\octane\install\initserver.bat
```

2. Check the **C:\octane\log\wrapper.log** file. If you do not see the "Server is ready!" message, correct the errors shown in the log.

 **Caution:** Do not use ALM Octane until you have completed ["Upgrade spaces in ALM Octane" on the next page](#).

Configure and upgrade cluster nodes

 **Caution:** Do not use ALM Octane until you have completed ["Upgrade spaces in ALM Octane" on the next page](#).

After the upgrade on the first node has completed successfully, you can then upgrade the remaining nodes in a cluster.

1. Copy **setup.xml** and **octane.yml** to each node.
2. Run **initserver.bat** on each additional node to install and initialize ALM Octane:

```
C:\octane\install\initserver.bat
```

For details, see "[Cluster installation \(optional\)](#)" on page 50.

Upgrade spaces in ALM Octane

After upgrading, log into ALM Octane as the site admin to upgrade each space.

1. In a browser, navigate to **<ServerURL>:<port>/ui?site**.
2. Log in as the space admin, with the user name and password you provided in the **setup.xml** file.
3. Click **Site** and then click the **Spaces** tab.
4. Select the space and click **Upgrade**.

Upgrade is available only if the space needs to be upgraded.

Click **Refresh** to see the updated status for the space.

Note: Upgraded spaces are, by default, isolated. To work with shared spaces, create new spaces.

5. Individual workspaces are upgraded in the background. In **Settings > Spaces**, click **Background Jobs** to track the progress of the workspace upgrades.

Note: Until all of the background jobs have completed, some data may be unavailable in trend graphs.

For details on upgrading the space, see the topic about upgrading spaces in the *ALM Octane Help Center*.

Restart all Jetty servers

After upgrading the spaces in Settings, clear caches:

1. Stop all Jetty servers.
2. Restart each Jetty server.

Note: Make sure all Jetty servers are stopped at the same time before restarting even one of them.

After the upgrade

After the upgrade has completed successfully:

- The space status becomes **Active**.
- The space version is updated to the current version.

Bulk update data access control

Note: This section is relevant only if you want to apply data access control for the first time to an upgraded system.

Follow the instructions in the *Set up data access* topic in the *ALM Octane Help center*. When you reach the *Assign data access categories to items* section, use the **Bulk Update** option to assign data access categories to items, so that all the items are accessible only to the relevant roles.

Next steps:

- Update mandatory configuration parameters, such as SMTP_NOTIFICATION_SENDER_EMAIL. See The topic about configuration parameters in the *ALM Octane Help Center*.
- Download the newest IDE plugins for this ALM Octane version. See the topic about IDE integrations in the *ALM Octane Help Center*.
- If you work with the REST API, you might want to check if any API resources have been deprecated. While the deprecated resources are supported for a while, we recommend that you start updating your code so that you use the resource aliases instead. To see deprecated resources for a particular version, see the corresponding REST API example and how to use the interactive API client in the *ALM Octane Developer Help*
- ["Rollback" below](#)

Rollback

This section describes how to roll back after upgrading an on-premises ALM Octane server. This may be necessary if for some reason the upgrade fails or performance is slow.

Depending on when you want to roll back, there are different steps to perform.

In this topic:

- ["After the upgrade's setup validation phase" on the next page](#)
- ["After site schema has been upgraded" on the next page](#)
- ["After space schema has been upgraded" on page 76](#)
- ["After upgrade completed" on page 76](#)
- ["After upgrading cluster nodes" on page 77](#)

After the upgrade's setup validation phase

You can roll back after the upgrade's setup validation phase, whether it passed or failed.

If the upgrade reached setup validation, the following have been modified:

- Previously-deployed files
- **setup.xml** and **octane.yml** configuration files

To roll back the deployed files, including the setup.xml, and octane.yml files

1. Back up the **setup.xml** file, the **octane.yml file**, and the folder in which you stored the repository, such as **C:\octane\repo**, if it is located inside the installation folder.
2. Uninstall the new ALM Octane version using Windows **Add/Remove Programs**. For details, see ["Uninstall" on page 95](#).
3. Install the previous ALM Octane version. For details, see ["Installation" on page 23](#).
4. Copy back the **setup.xml**, and **octane.yml** files.
5. If necessary, copy back the folder in which you stored the repository, such as **C:\octane\repo**.
6. Re-initialize the ALM Octane service. For details, see ["Start the ALM Octane server manually" on page 78](#).

After site schema has been upgraded

You can roll back after the upgrade's site schema have been upgraded.

If the upgrade upgraded the site schema, the following has been modified:

- Previously-deployed files
- **setup.xml** and **octane.yml** configuration files
- The site schema

To roll back the site schema

1. Stop the ALM Octane service.
2. Back up the **setup.xml** file, the **octane.yml file**, and the **C:\octane\repo** folder, if it is located inside the installation folder.
3. Revert to a backup of the site schema.
4. Uninstall the new ALM Octane version using Windows **Add/Remove Programs**. For details, see ["Uninstall" on page 95](#).
5. Install the previous ALM Octane version. For details, see ["Installation" on page 23](#).
6. If necessary, copy back the **C:\octane\repo** folder.
7. Revert to backups of **setup.xml** and **octane.yml** configuration files.
8. Re-initialize the ALM Octane service. For details, see ["Start the ALM Octane server manually" on page 78](#).

After space schema has been upgraded

If the upgrade upgraded the site schema, the following have been modified:

- The space schema
- Elasticsearch indexes
- ALM Octane repository files

Follow the steps for one of the following options.

Rollback option	Steps
To roll back changes to the space schema	<ol style="list-style-type: none">1. Open the backup of the space schema.2. Open the backup of Elasticsearch indexes.3. Open the repository backup for this specific space.4. Fix what caused the upgrade to fail.5. Reset the following for the space within the site schema:<ol style="list-style-type: none">a. Open the SHARED_SPACE table.b. Find the record for the shared space. You can search for the SP_NAME.c. Set the SP_STATUS to ACTIVE.d. Set the SP_VERSION to the original version number before upgrading.6. Upgrade again.
To roll back the entire upgrade	Follow the steps for "To roll back the site schema" on the previous page .

After upgrade completed

If the upgrade completed successfully, the following have been modified:

- Previously-deployed files
- **setup.xml** and **octane.yml** configuration files
- The site schema
- The space schema
- Elasticsearch indexes
- ALM Octane repository files

To roll back the entire upgrade

1. Follow the steps for ["To roll back the site schema" on the previous page](#).
2. Follow the steps for ["To roll back changes to the space schema" above](#) for each space.

After upgrading cluster nodes

If you upgraded additional cluster nodes, the following has been modified on the cluster nodes:

- Previously-deployed files
- **setup.xml** and **octane.yml** configuration files

To roll back the previously-deployed files

1. Uninstall the current version. For details, see ["Uninstall" on page 95](#).
2. Install the previous version on a node.
3. Run **initserver.bat** on each additional cluster node. For details, see ["Cluster installation \(optional\)" on page 50](#).
4. Re-initialize the ALM Octane service on each cluster node. For details, see ["Start the ALM Octane server manually" on the next page](#).

See also:

- ["Management" below](#)

Management

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

This section includes:

- [Start the ALM Octane server manually](#) 78
- [Handle database-related issues](#) 78
- [Configure trust on the ALM Octane server](#) 79
- [Configure a secure connection to the ALM Octane server \(Jetty\)](#) 80
- [Using exception files for manual database changes](#) 81

Including these management tasks, you can also set configuration parameters to define how your site operates. Configuration parameters for the site are set using Settings. For details, see the topic about configuration parameters in the *ALM Octane Help Center*.

See also:

- Linux [Prerequisites](#) or Windows "[Prerequisites](#)" on page 15
- Linux [Architecture](#) or Windows "[Architecture](#)" on page 5
- Linux [Installation flow](#) or Windows "[Installation flow](#)" on page 13

Start the ALM Octane server manually

When installing ALM Octane, the ALM Octane server is started as part of running **initserver.bat**.

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](#)" on the previous page

Handle database-related issues

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

In this topic:

- "[Change site schema settings and reinitialize](#)" below

Change site schema settings and reinitialize

If you need to make changes to the site schema settings, make the changes in the **setup.xml** file.

1. Obtain the names of the indexes related to your instance of ALM Octane in the **sharedspace_logical_name.txt** in the **C:\octane\server\conf** folder.
2. Delete the database site schema.
3. Delete the repository.
4. Delete the **mqm_<sp_logical_name>** index from Elasticsearch. From the command prompt on the

ALM Octane server, run:

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

5. Run **initserver.bat** with the site action **CREATE_NEW** in the **setup.xml** file to create a new site schema.

```
C:\octane\install\initserver.bat
```

 See also:

- ["Management" on page 77](#)

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 initializing the ALM Octane server by running **initserver.bat**.

In this topic:

- ["Configure trust" below](#)

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:\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.

Next steps:

- ["Management" on page 77](#)

Configure a secure connection to the ALM Octane server (Jetty)

This topic describes how to configure a secure connection to the ALM Octane server with Jetty.

Note: ALM Octane uses the TLSv1.2 secure protocol.

In this topic:

- ["Configure the connection" below](#)
- ["Configure a secure connection to the ALM Octane server \(Jetty\)" above](#)

Configure the connection

1. Obtain the server certificate issued to the name of this server in java keystore format (.jks) issued to the fully qualified domain name of ALM Octane server. It must contain a private key and the certificate authority that issued it. For details on creating certificates using the Certificate Authority, see [Software Self-solve knowledge base article KM02707977](#).
2. Copy your keystore file to the C:\octane\conf folder. Name the file **keystore.jks**.
3. Run C:\octane\install\enabless1.bat, supplying the certificate password as a parameter to the script.

Limitations

Note the following limitations:

- 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.

See also:

- ["Management" on page 77](#)

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.

In this topic:

- ["Overview" below](#)
- ["Define exception files" below](#)
- ["Set up use of the exception file" on page 83](#)

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.

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 **setup.xml** file.

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

MqmExceptionsSiteAdminPath	The exception file for the site. C:\temp\site_admin\mqm_exception.xml
MqmExceptionsSharedSpacePath	The exception file for the default space. C:\temp\shared_space\mqm_exception.xml

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 **C:\octane\conf\setup.xml** file in the repository folder, add or modify these two settings using an editor:

The exception file for the site	C:\octane\repo\storage\schema\maintenance\exceptions\site_admin\mqm_exception.xml
The exception file for the new space	C:\octane\repo\storage\schema\maintenance\exceptions\shared_space\mqm_exception.xml

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	C:\octane\repo\storage\schema\maintenance\exceptions\site_admin\mqm_exception.xml
The exception file for the new space	C:\octane\repo\storage\schema\maintenance\exceptions\shared_space\mqm_exception.xml

2. In ALM Octane Settings area, add the space using an existing schema. For details, see the topic about creating spaces for a site in the *ALM Octane Help Center*.
3. Check that you have proper access to the space.

 **See also:**

- ["Configure initial site settings" on page 27](#)
- ["Management" on page 77](#)

Best practices

Here are some best practices you may want to consider adopting during or after installation.

This section includes:

- [Best practices: Deploying ALM Octane](#)85
- [Best practices: Backing up ALM Octane data](#)86
- [Best practices: Maintenance](#)88
- [Best practices: Setting up spaces and workspaces](#)90

See also:

- Linux [Prerequisites](#) or Windows "[Prerequisites](#)" on page 15
- Linux [Architecture](#) or Windows "[Architecture](#)" on page 5
- Linux [Installation flow](#) or Windows "[Installation flow](#)" on page 13

Best practices: Deploying ALM Octane

This topic describe the main components of the ALM Octane architecture and provides best practices and recommendations for enterprise deployment of ALM Octane on-premises.

In this topic:

- ["Overview " below](#)
- ["Architecture" below](#)
- ["General guidelines" below](#)
- ["Minimal and suggested requirements" on the next page](#)

Overview

ALM Octane is available:

- As a service offered by Micro Focus SaaS.
- As an on-premises installation as a compressed package (**rpm** or **zip**).

Architecture

ALM Octane includes the following main components:

- Database
- Elasticsearch
- ALM Octane server

Each component should reside on separate, dedicated machine(s). Each component can be scaled using clustering to provide better performance, load balancing, and fault tolerance.

For details on the ALM Octane architecture, see the architecture diagrams in the *ALM Octane Installation Guide* or the ALM Octane Help Center.

General guidelines

While planning the enterprise deployment, consider the following:

- The capacity for production environments is hard to assess due to unknown patterns of behavior. Will testing be manual or automatic? Will there be a large backlog with a considerable or minimal number of tasks? How many workspaces are needed? And so on.
- Our recommendations are based on Micro Focus generic assumptions. Reassess the environment

after 1-2 years of full production usage.

- The specifications provided here do not relate to the installation and configuration of 3rd party software. See vendor documentation to prepare clustered installations of the database and Elasticsearch.
- While each component can be clustered, clustering does not necessarily improve performance linearly. This is because performance depends on the types of operations your users perform. However, it is important to design the environment in such a way that you can add more cluster nodes later.

Minimal and suggested requirements

For the most up-to-date list of requirements, see the system requirements provided in the ALM Octane Help Center.

See also:

- ["Best practices" on page 84](#)

Best practices: Backing up ALM Octane data

This topic provides best practices and recommendations for backing up ALM Octane and all its components.

In this topic:

- ["Overview" below](#)
- ["The process" on the next page](#)
- ["Best practices" on page 88](#)

Overview

ALM Octane stores its information in the following components:

- **Your relational database (either Oracle or SQL Server).** This is where the most important system data are located. The relational database is the most important component of the backup.
Database systems support hot backup procedures and provide the ability to restore operations to the last second before the system crash.
- **Elasticsearch.** Elasticsearch stores trend data, run history, search information, and additional miscellaneous items.
You can take periodic snapshots of Elasticsearch data.
- **The repository folder on your file system.** ALM Octane includes its own file system repository where attachments, manual scripts and other artifacts are kept. The default location for this folder is:
 - Linux: **`/opt/octane/repo`**

- Windows: **C:\octane\repo**

You can take periodic snapshots of repository data.

The process

To fully back up ALM Octane, back up all its components: the relational database, Elasticsearch, and the repository folder. Store each backup in a separate location to allow for (disaster) recovery.

Order matters

- Time may elapse as you back up each of these components. In terms of time difference tolerance, the time as specified in the relational database is used as the determining factor. When you restore ALM Octane, it is the data and timestamps stored in the relational database that users see. Keep this in mind when restoring.
- If you backed up your relational database, added files, and only then backed up the repository, the files exist after restore, but ALM Octane does not see any associations to them, and eventually deletes them.

Conversely, if you backed up the repository, added files, and only then backed up the relational database, ALM Octane might report that you have some broken associations, as the files do not exist in the repository while ALM Octane tries to find them.

Frequency of backups

While database systems, such as Oracle and SQL Server, support hot backup procedures and provide the ability to restore operations to the last second before the system crash, it is only possible to take a periodic snapshot of the Elasticsearch and ALM Octane repository.

Therefore, how often you should back up is determined by the amount of down time your site can tolerate. If the amount of tolerated time is one day (meaning, the company is fine with the ability to restore the operation to the state of 24 hours ago), the suggested backup frequency could be defined as one day. If the amount of tolerated time is 12 hours, backups should run every 12 hours.



Example: ALM Octane operations on SaaS are backed up every 4 hours. In most cases, hot backups and dumps/snapshots should then be either moved to a separate location or put on removable media for storage.

Backing up the relational database

Use the database's backup mechanism and save the resulting files and folders.

Open files do not pose a problem during the backup, as most files are not locked by ALM Octane.

Best practices

The relational database is the most important component in the backup.

General

- Back up each component as closely as possible, one after the other.
- Back up ALM Octane during quiet times to minimize missing files, broken file associations, and time inconsistencies between the three components.

Recommended order for backing up components

Here are suggested guidelines and the sequence of backup actions to take.

1. Always back up the database first. Use the database vendor's, or commercially-available, tools to perform a hot backup (such as Oracle RMAN). We recommend that you take a snapshot (dump) before performing any major operations on the database, such as an upgrade, data migration (such as from Agile Manager to ALM Octane), massive import, and so on.
2. Back up Elasticsearch next. Elasticsearch is a NoSQL database geared toward fast textual indexing and search. You can take a snapshot of the Elasticsearch index periodically using REST API commands from any programming language (for example, JavaScript). Kibana is one tool recommended by Elastic for issuing REST API commands.

See <https://www.elastic.co/guide/en/elasticsearch/reference/current/modules-snapshots.html> on the Elasticsearch site.

To back up properly in a clustered Elasticsearch environment, attach shared storage to which snapshots from each node can be saved.

3. Lastly, back up the ALM Octane repository. Make a complete backup using operating system capabilities (**tar**, **zip**) or commercially-available tools.

See also:

- ["Best practices" on page 84](#)
- ["Disaster recovery" on the next page](#)

Best practices: Maintenance

To maintain uninterrupted operations, we recommend you follow the following best practices for the ALM Octane production environment.

In this topic:

- ["Overview" on the next page](#)
- ["Periodic maintenance" on the next page](#)
- ["Disaster recovery" on the next page](#)

Overview

These best practices help maintain the following main components that are necessary for proper functioning of ALM Octane:

- The ALM Octane application server
- The Elasticsearch server
- The database server

Periodic maintenance

Periodic maintenance includes upgrading to new versions of the product, including patches. This involves:

- Downloading the appropriate version build from Micro Focus Software Self-service Online.
- Deploying the package.
- Performing database upgrade steps.

Before upgrading to a new build or patch, make sure to:

1. Back up the database.
2. Back up (meaning, take a snapshot of) the Elasticsearch index.
3. Back up the ALM Octane repository file system.
4. Back up the ALM Octane configuration files (which are located at **/opt/octane/conf** by default).

For details on backing up, see ["Best practices: Backing up ALM Octane data" on page 86](#).

For details on upgrading, see the upgrade procedure in the *ALM Octane Installation Guide*.

Disaster recovery

ALM Octane can be deployed in a cluster to allow for uninterrupted operation. In fact, each component can be scaled out:

- Database and Elasticsearch, according to vendor instructions.
- ALM Octane cluster guidelines can be found in the *ALM Octane Installation Guide*.

Having backup procedures in place allows for data integrity and completeness.

In addition, ALM Octane does not lose data at a time of crash, because data is kept in database. All asynchronous jobs are persistent.

See also:

- ["Best practices" on page 84](#)
- ["Best practices: Backing up ALM Octane data" on page 86](#)

Best practices: Setting up spaces and workspaces

This topic provides best practices and recommendations for setting up spaces and workspaces in ALM Octane.

In this topic:

- ["Overview " below](#)
- ["Planning how to set up spaces" on the next page](#)
- ["Planning how to set up spaces" on the next page](#)

Overview

This overview provides basic information about the various types of spaces in ALM Octane and how to work with them.

Terms

Site	Top level container. Allows the management of the different spaces created in ALM Octane as well as a place to carry administrative tasks and manage users.
Space	Top level logical container. Provides absolute isolation of data. A space is the highest container level that allows data sharing and interaction. A space allocates its own resources when created, such as relational database schema, Elasticsearch indexes, and the repository location.
Workspace	A working container. A user always works in the context of a specific workspace. A workspace is always contained in a shared space and provides logical isolation of data and settings. The level of isolation is defined by the type of shared space created.

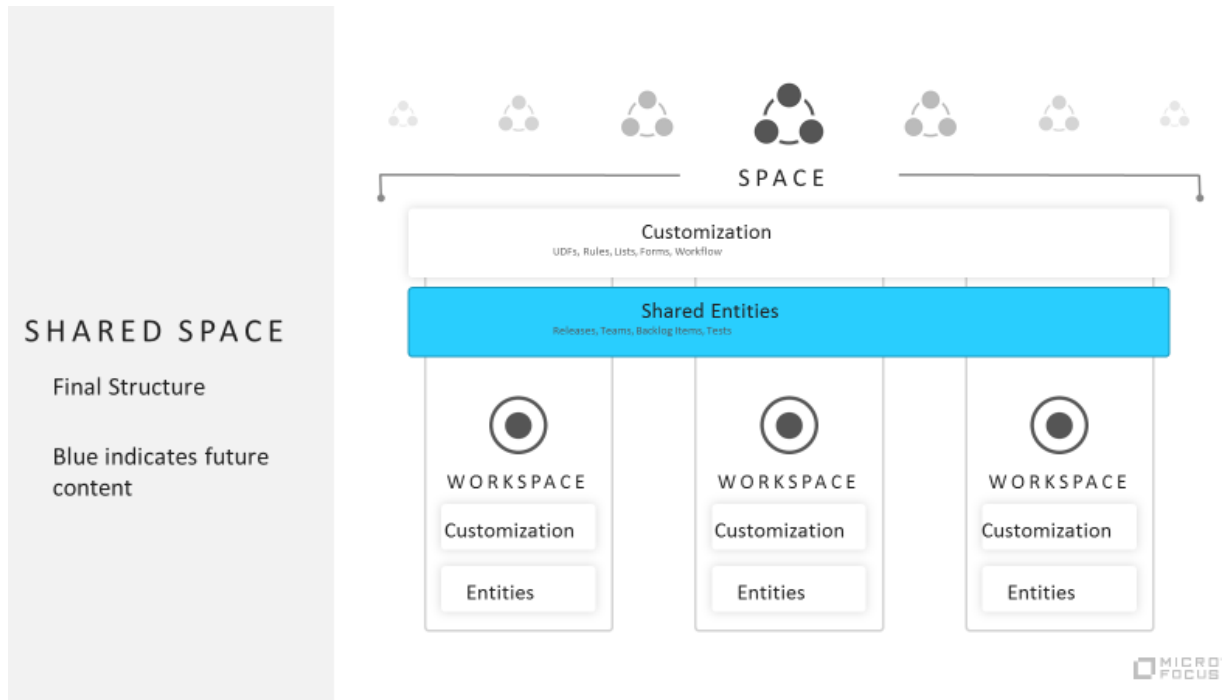
For details about the site and spaces, see the information about spaces in the ALM Octane.

Types of spaces

ALM Octane Enterprise edition provides the following types of spaces: Shared and Isolated.

Shared space (Enterprise edition)	Workspaces share customization and can share data. Cross workspace reporting is possible. Some entities may be defined as global and be viewed across all workspaces.
---	---

<p>Isolated space</p> <p>(Pro and Enterprise editions)</p>	<p>Each workspace defines its own customization. No sharing between workspaces. A user can be assigned to multiple workspaces and seamlessly switch between them.</p> <div data-bbox="423 310 1411 436" style="background-color: #e6f2e6; padding: 5px;"><p>Note: Pro edition only allows creation of isolated spaces. Shared spaces are an enterprise level feature.</p></div>
---	--



Planning how to set up spaces

This topic provides strategies for planning spaces (both isolated and shared) in your ALM Octane deployment.

Space strategy overview

When planning your ALM Octane deployment, it is important to plan how to break down your projects into a structure that provides you with the best experience for your teams.

Generally, unless there is an actual need for complete isolation of workspaces, use shared spaces (instead of isolated spaces). The use of shared spaces allows you to better scale out ALM Octane as your projects grow.

Consider the following factors.

Amount of interaction and data-sharing between projects

If you have projects that have close interaction and work together frequently, consider putting them either in the same workspace or in different workspaces under the same shared space.

This best practice is relevant in both this use case, sharing data, and also the use case for having similar processes and shared customization. For more suggestions about working with similar process and shared customization, see ["Projects that have shared processes and policy" below](#).

When trying to evaluate and understand interaction level between the projects, and the need to share data, relate to factors such as team collaboration level, dependencies among teams, common releases, integration among the applications, and so on.

The level of interaction between teams is the most major factor for deciding whether teams and products should be in the same workspace. For details, see ["Planning how to set up spaces" on the previous page](#).

If you define teams and products in separate workspaces, knowing that the teams and products need some level of interaction that require dependencies between entities and sharing of data, these workspaces should reside within the same shared space. Workspaces that reside within the same shared space are able to more easily share entities and set dependencies between entities in the following ways:

- Define shared entities at the shared space level.
- Move entities from one workspace to another.
- Define dependencies between entities on different workspaces within the same shared space.

Projects that have shared processes and policy

If you are an enterprise customer, you can enforce your process and align organizational standards to all workspaces within a shared space by customizing at the shared space level. This customization is achieved using business rules, common fields, workflow, lists, and so on.

ALM Octane also provides customization on the workspace level, so the teams and products don't have to be fully aligned. However, defining the main processes and standards at the shared space level is advantageous because not only does it apply to all workspaces, you can also add additional processes, definitions, and standards for specific projects in specific workspaces. This provides flexibility.

If you have sets of workspaces that do not need any interaction, the recommendation is to separate the sets of workspaces into different shared spaces, and manage the common customizations on the different shared spaces accordingly.

Note: Managing common customization for large number of workspaces might result in a very complicated customization at the shared space level that is hard to manage and eventually can also cause performance degradation. If the shared space admin does want to have a significant portion of the customization shared, the more workspaces there are with greater variance, the more work the shared space admin needs to do to manage the variance.

Make sure that the customization at the shared space level is relevant and needed for all workspaces. Additional flexibility can be done at the customization of each workspace, but if there is a need for common customization for partial set of workspaces within the same shared space, then probably these workspaces should be in a different shared space.

Note: Same applies also to management of shared assets. If there are too many variations between the workspaces and the need for different shared entities, it results in a large number of shared assets which are hard to manage.

Cross-workspace reporting

If there is a need to track projects managed in different workspaces, having these workspaces on the same shared space enables cross-workspace reporting, which reflects the data from different workspaces in the ALM Octane dashboard. For example, if two projects share the same release and you want to understand the progress of each project in the release, put each project in its own workspace, and make sure both workspaces are under the same shared space,

Cross-workspace reporting is also possible even if the workspaces are under different shared spaces. You can do this by using OData, which extract workspaces data to external BI tools. For details, see the information about OData support for extended reporting in the ALM Octane Help center.

Data isolation

If a project requires absolute data isolation, define the project in a workspace in its own isolated space. This ensures that there is no way to inadvertently expose confidential information between projects.

Disaster recovery planning (DRP)

Each space is stored in a different database schema (Oracle) or database (SQL Server).

Note: For the purposes of this discussion, we will use the Oracle terminology.

Workspaces within the same space share the same database schema as the space. This means that backup and recovery can be done over an entire space, and it includes all its workspaces.

Recovery therefore recovers all workspaces in a space. You cannot recover just one workspace in a space.

Planning how to set up workspaces

This topic provides strategies for planning workspaces in your ALM Octane deployment.

Workspace strategy overview

Similar to the strategy for setting up spaces, consider how to partition projects within a space. The factors to consider are similar to the space strategy parameters, but on a smaller scale.

If the projects are tightly intertwined, and a large portion of the data needs to be used by different teams in these projects, the projects should reside within the same workspace to allow ease of sharing of data.

You can make sure that each project member only sees the information that is relevant in the following ways:

- Use basic filtering to partition data within a workspace.
- Assign and customize roles.
- Customize module access.
- Set up data access.

Consider the following factors.

Sharing of data between teams

The main factor for deciding whether teams and projects should be in the same workspace or separate workspaces is the level of shared data that is common for the teams. If teams share the same release planning and content, or have strong dependencies on different entities, these teams and projects should probably share the same workspace.

Data isolation

Different workspaces provide data isolation. If there is a need to isolate data between the different teams and projects, this probably indicates that these teams and projects should be managed in different workspaces.

ALM Octane provides data access capabilities, but these should be used for specific cases when some entities need to be hidden for certain users and teams, and not in the case of most data needing to be hidden. If most data needs to be hidden between teams, use different workspaces.

Different processes

All workspaces within the same shared space inherit the common customization from the shared space level.

You can customize each workspace even further, on top of the shared customization for the space. This enables you to define additional processes relevant for the workspace level only. If there is a need for different customization at the workspace level for compliance with different processes, and there is no need to share data, we recommend that you define these projects and teams in different workspaces.

Performance considerations

Try to break down your spaces into as many workspaces as possible as this helps ALM Octane perform better and makes searching for data, and concentrating on your tasks, easier. The best practice is to have many small workspaces in the same space instead of a few, very big workspaces.

See also:

- ["Best practices" on page 84](#)

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 23](#)

Send Us Feedback



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

Send your email to: docteam@microfocus.com

