opentext™

OpenText™ Application Quality Management

Software version: 26.1

Installation Guide

Go to Help Center online
https://admhelp.microfocus.com/alm/

Document release date: March 2026

Send Us Feedback

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

Send your email to: admdocteam@opentext.com

Legal Notices

Technology and Architecture

OpenText Application Quality Management is an enterprise-wide application that is based on Java 2 Enterprise Edition (J2EE) technology. J2EE technology provides a component-based approach to the design, development, assembly, and deployment of enterprise applications.

Understanding the Components

An OpenText Application Quality Management system contains the following components:

- **Client components.** When you open Application Lifecycle Management or Site Administration on your client machine, client components are downloaded to the machine. Client components interact with each other using .NET and COM technologies. The client communicates with the server over HTTP/S.
- **Server/Application server.** Client requests are dispatched by servlets to the deployed server. OpenText Application Quality Management comes with a built-in application server called the Application Server.

  The deployed application contains Application Lifecycle Management, Site Administration, and associated files which are packaged into a Web Application Archive (WAR) file. Client requests from OpenText Application Quality Management are dispatched to the deployed application.

  The Java Database Connectivity (JDBC) interface is used to communicate between the application server and database server(s).

  The server can run on a Windows or Linux platform.
- **Database server(s).** The database server stores three types of schemas:
  - **Site Administration schema.** Stores information related to the system, such as domains, users, and site parameters. A row exists in this schema

for each project you create.

Irrespective of how you configure your system, there is always only one Site Administration schema.

- **Lab_Project.** Stores lab information related to managing functional and performance testing on remote hosts, LoadRunner Enterprise server data, and licenses. There is always only one Lab_Project schema.
- **Project schemas.** Stores project information, such as entity data and user data. A separate schema exists for every project you create.

  By default, the project schemas are created on the same database server as the Site Administration schema. These default project schemas are useful for smaller setups. However, if you are working with a large number of projects or with a small number of huge projects, it may be advisable to define additional database servers solely for storing project schemas. You define additional servers in the Site Administration DB Servers tab.

The schemas can reside on an Oracle or on a Microsoft SQL server.

> **Note:** To improve system performance, it is advisable that the application server and the database server be installed on separate machines and be connected over LAN.

- **Project repository.** Stores all files to be used by all the projects in the system. For example, **.xml** files, templates, and attachments. By default the repository is located on the same machine as the application server, which is useful for smaller setups. For larger organizations however, or when working in a clustered environment, it is advisable to install the repository on a dedicated machine.

  When working in a clustered environment, the repository must be accessible by all nodes.
- **Load balancer.** When working with a load balancer, client requests are transmitted to the load balancer and distributed according to server

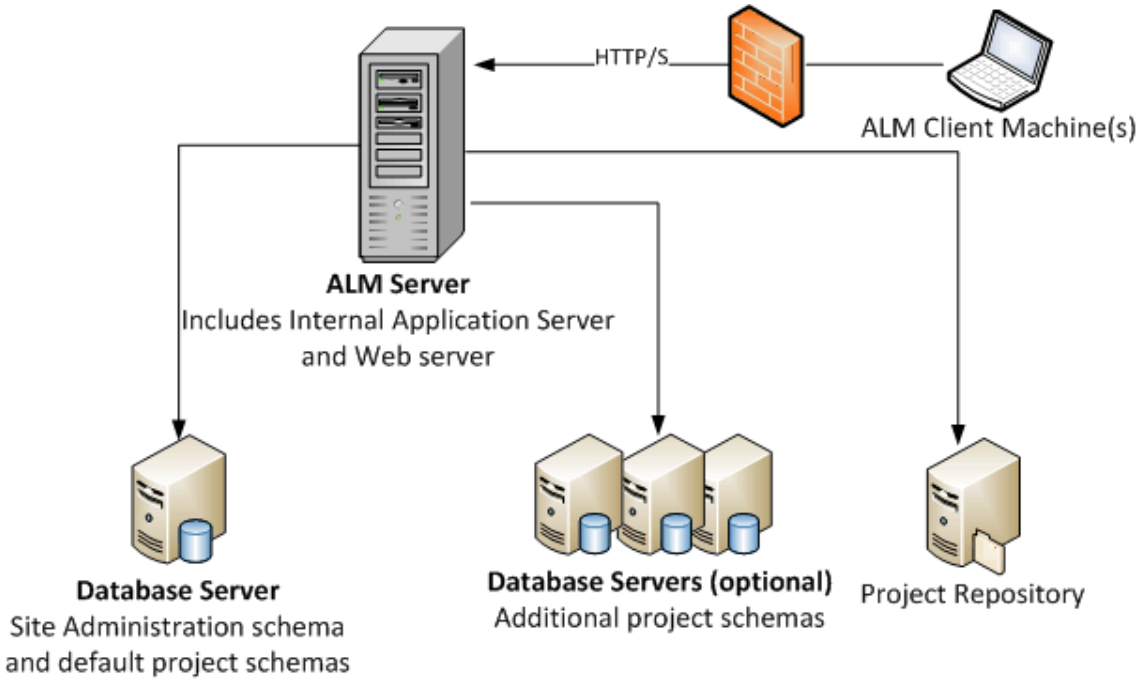
availability within the cluster.

- **Tanuki wrapper.** A Java service wrapper that allows OpenText Application Quality Management to be installed and controlled like a native Windows Service. It also includes advanced fault detection software to monitor OpenText Application Quality Management.

Example of Basic Configuration

In the basic OpenText Application Quality Management configuration, the Jetty application server and the web server are embedded with the installation and installed on the same machine.

The following diagram illustrates a basic system configuration:



To enhance security in this configuration:

- Enable SSL on the Jetty and make it required.

  Alternatively, install an Apache or IIS web server acting as a reverse proxy in front of the server and configure SSL on the reverse proxy server. This

protects the server and uses the IIS or Apache security related features to enhance security.

For information on enabling SSL for all interactions with IIS, see the IIS documentation. SSL must be enabled for the entire IIS web server under which you install the ALM applications.

For information on enabling SSL for all interactions with Apache, see the Apache documentation.

- Use a firewall and close access to all incoming traffic except for the https/http port used by OpenText Application Quality Management.

Example of Clustered Configuration

Within the J2EE framework, OpenText Application Quality Management supports clustering. A cluster is a group of application servers that run as if they were a single system. Each application server in a cluster is referred to as a node.

Clusters provide mission-critical services to ensure maximum scalability. The load balancing technique within the cluster is used to distribute client requests across multiple application servers, making it easy to scale to an infinite number of users.

Take the following into consideration when setting up a clustered environment:

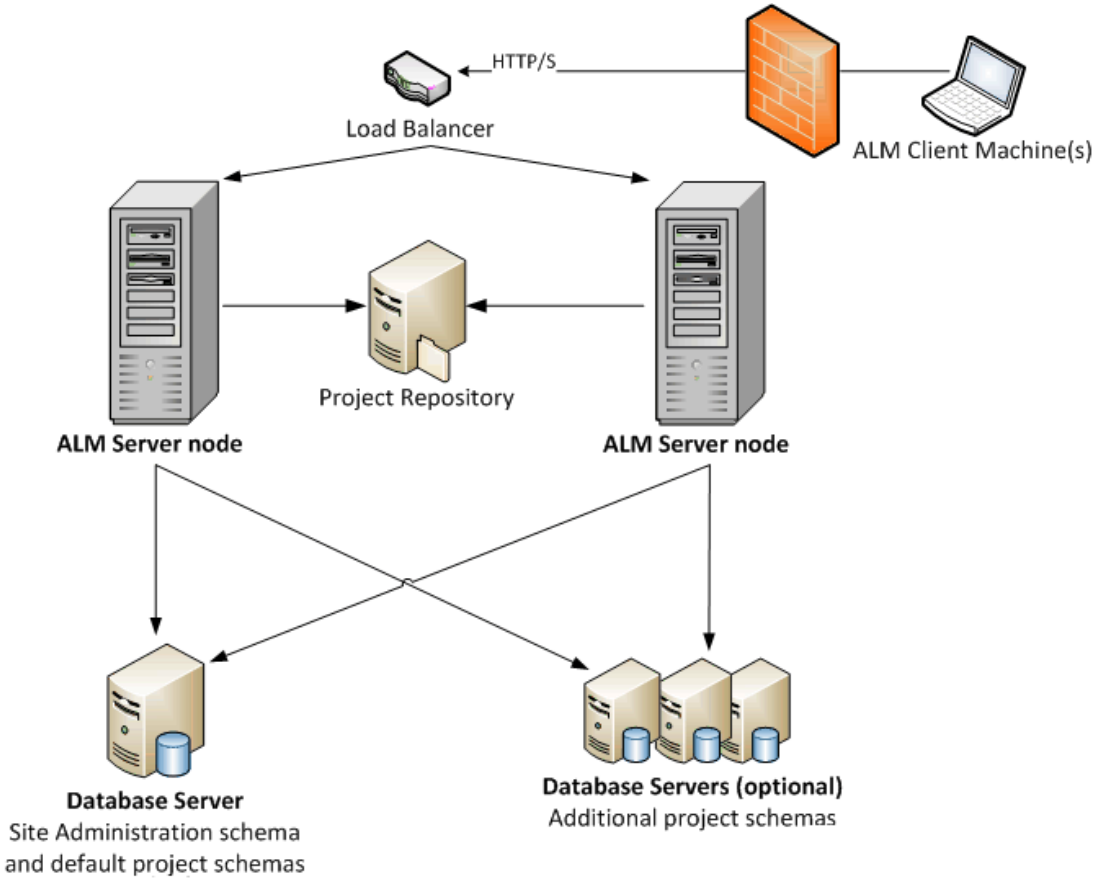
- All nodes must have access to the database server on which the Site Administration database schema resides.
- All nodes must have access to all database servers.
- All nodes must have access to the repository. By default the repository is located on the first node in the cluster, and therefore all other nodes must have access to the first node. If you install the repository on a dedicated machine, each node must have access to that machine.

- The load balancer must be configured with the health monitor, using the following KeepAlive uniform resource identifier (URI):
  - `Send String: GET /qcbin/servlet/tdservlet/`
  - `Receive String: up and running`
- The load balancer must be configured with session persistency. Set the persistency to **sticky session enabled** or **destination address affinity**, depending on the load balancer.

To enhance security in this configuration:

- Require SSL for the ALM virtual IP on the load balancer.
- Use a firewall on each ALM server to block access to all incoming traffic except for the http port (8080) or https port (8443) used by OpenText Application Quality Management.
- If you have external clients connecting to the deployment from outside the corporate firewall, place an Apache or IIS web server as a reverse proxy in front of the corporate firewall behind which the servers are deployed, and require SSL on the reverse proxy.

The following diagram illustrates a clustered system configuration:



How to install and upgrade

This section presents an overview of installation and upgrade processes.

Installing and upgrading consists of the following steps:

1. **Check that you meet all relevant installation prerequisites.**

   Before beginning the actual installation procedure, check that your server machine's operating system, your database server, and your client machines, all meet the prerequisite criteria for working with 25.1. For details, see "Installation prerequisites" on page 33.

2. **(Upgrading) Check that you meet all relevant upgrade prerequisites.**

   If you are upgrading from an earlier version of OpenText Application Quality Management/Quality Center, it is important to carefully consider how to configure your new OpenText Application Quality Management system. This guide provides a suggested system configuration for upgrading projects from your existing system. Follow the suggested configuration as much as possible.

   Before beginning the installation, verify and repair all projects in the existing system, and then back up the projects, the database, and the repository.

   If you plan to upgrade a copy of the Site Administration database schema, you need the Confidential Data Passphrase that was used in the existing installation, and you must manage changes to the existing schema (if any).

   For details, see "Pre-Installation project upgrade steps" on page 63.

3. **Install 25.1.**

   Install 25.1 on your server machine. The installation is guided by a step-by-step wizard. For details, see "Installation and configuration" on page 76.

4. **(Upgrading) Upgrade projects from your existing OpenText Application Quality Management system.**

Upgrade your existing projects to 25.1 based on your system configuration. Note the project repository migration options. For details, see "Project upgrade" on page 176.

See also:

- "New installation" below
- "Upgrade with new schema" on page 12
- "Upgrade with copied schema" on page 15
- "Upgrade with same server" on page 18
- "Upgrade with same database server" on page 21

New installation

This section details the steps for installing on Window and Linux.

New installation - Windows

The table below lists the steps for the following scenario:

- **Installing OpenText Application Quality Management for the first time**
- Windows
- SQL database

Installation Step	Instructions
Prerequisites	• "Prerequisites: Windows Operating Systems" on page 36 • "Prerequisites: Microsoft SQL Database Servers" on page 54 • "Prerequisites: General" on page 58 • "Prerequisites: Client-side" on page 60

Installation Step	Instructions
Installation	"Install on Microsoft Windows systems" on page 76
Start OpenText Application Quality Management	"Starting the system" on page 123
Manage OpenText Application Quality Management	• "Manage the application server" on page 137 • "Customize system files" on page 166
Troubleshoot the Installation	"Troubleshooting the installation" on page 222

New installation - Linux

The table below lists the steps for the following scenario:

- **Installing OpenText Application Quality Management for the first time**
- Linux
- Oracle database

Installation Step	Instructions
Prerequisites	• "Prerequisites: Linux Operating Systems" on page 40 • "Prerequisites: Oracle Database Servers" on page 44 • "Prerequisites: General" on page 58 • "Prerequisites: Client-side" on page 60
Installation	"Install on Linux systems" on page 95
Start OpenText Application Quality Management	"Starting the system" on page 123

Installation Step	Instructions
Manage OpenText Application Quality Management	• "Manage the application server" on page 137 • "Customize system files" on page 166
Troubleshoot the Installation	"Troubleshooting the installation" on page 222

Upgrade with new schema

This section details the steps for upgrading with a new schema on Windows and Linux.

Windows upgrade

The table below lists the steps for the following scenario:

- Upgrading OpenText Application Quality Management to a new version
- Windows
- SQL database
- New OpenText Application Quality Management server
- New database server
- New Site Administration schema

Installation Step	Instructions
Prerequisites	• "Prerequisites: Windows Operating Systems" on page 36 • "Prerequisites: Microsoft SQL Database Servers" on page 54 • "Prerequisites: General" on page 58 • "Prerequisites: Client-side" on page 60

Installation Step	Instructions
Project Upgrade Prerequisites	• "Back up projects in existing installation" on page 66 • "Verify domains and projects" on page 67 • "Upgrade preparation troubleshooting" on page 190 • "Repair domains and projects" on page 67 • "Restore backed up projects and repositories" on page 68
Installation	"Install on Microsoft Windows systems" on page 76
Start OpenText Application Quality Management	"Starting the system" on page 123
Project Upgrade	"Project upgrade" on page 176
Manage OpenText Application Quality Management	• "Manage the application server" on page 137 • "Customize system files" on page 166
Troubleshoot the Installation	"Troubleshooting the installation" on page 222

Linux upgrade

The table below lists the steps for the following scenario:

- Upgrading OpenText Application Quality Management to a new version
- Linux
- Oracle database
- New OpenText Application Quality Management server
- New database server
- New Site Administration schema

Installation Step	Instructions
Prerequisites	• "Prerequisites: Linux Operating Systems" on page 40 • "Prerequisites: Oracle Database Servers" on page 44 • "Prerequisites: General" on page 58 • "Prerequisites: Client-side" on page 60
Project Upgrade Prerequisites	• "Back up projects in existing installation" on page 66 • "Verify domains and projects" on page 67 • "Upgrade preparation troubleshooting" on page 190 • "Repair domains and projects" on page 67 • "Restore backed up projects and repositories" on page 68
Installation	"Install on Linux systems" on page 95
Start OpenText Application Quality Management	"Starting the system" on page 123

Installation Step	Instructions
Project Upgrade	"Project upgrade" on page 176
Manage OpenText Application Quality Management	• "Manage the application server" on page 137 • "Customize system files" on page 166
Troubleshoot the Installation	"Troubleshooting the installation" on page 222

Upgrade with copied schema

This section details the steps for upgrading with a copied schema on Windows and Linux.

Upgrade with copied schema - Windows

The table below lists the steps for the following scenario:

- Upgrading OpenText Application Quality Management to a new version
- Windows
- SQL database
- New OpenText Application Quality Management server
- New database server
- Copying the existing Site Administration schema

Installation Step	Instructions
Prerequisites	• "Prerequisites: Windows Operating Systems" on page 36 • "Prerequisites: Microsoft SQL Database Servers" on page 54 • "Prerequisites: General" on page 58 • "Prerequisites: Client-side" on page 60

Installation Step	Instructions
Project Upgrade Prerequisites	• "Back up projects in existing installation" on page 66 • "Verify domains and projects" on page 67 • "Upgrade preparation troubleshooting" on page 190 • "Repair domains and projects" on page 67 • "Restore backed up projects and repositories" on page 68 • "Copy Site Administration database schema to the new database server" on page 68 • "Upgrade the Site Administration database schema" on page 69
Installation	"Install on Microsoft Windows systems" on page 76
Start OpenText Application Quality Management	"Starting the system" on page 123
Project Upgrade	"Upgrade projects" on page 185
Manage OpenText Application Quality Management	• "Manage the application server" on page 137 • "Customize system files" on page 166
Troubleshoot the Installation	"Troubleshooting the installation" on page 222

Upgrade with copied schema - Linux

The table below lists the steps for the following scenario:

- Upgrading OpenText Application Quality Management to a new version
- Linux
- Oracle database
- New OpenText Application Quality Management server

- New database server
- Copying the existing Site Administration schema

Installation Step	Instructions
Prerequisites	• "Prerequisites: Linux Operating Systems" on page 40 • "Prerequisites: Oracle Database Servers" on page 44 • "Prerequisites: General" on page 58 • "Prerequisites: Client-side" on page 60
Project Upgrade Prerequisites	• "Back up projects in existing installation" on page 66 • "Verify domains and projects" on page 67 • "Upgrade preparation troubleshooting" on page 190 • "Repair domains and projects" on page 67 • "Restore backed up projects and repositories" on page 68 • "Copy Site Administration database schema to the new database server" on page 68 • "Upgrade the Site Administration database schema" on page 69
Installation	"Install on Linux systems" on page 95
Start OpenText Application Quality Management	"Starting the system" on page 123
Project Upgrade	"Upgrade projects" on page 185
Manage OpenText Application Quality Management	• "Manage the application server" on page 137 • "Customize system files" on page 166
Troubleshoot the Installation	"Troubleshooting the installation" on page 222

Upgrade with same server

This section details the steps for upgrading on Windows and Linux with a the same OpenText Application Quality Management server.

Upgrade with same server - Windows

The table below lists the steps for the following scenario:

- Upgrading OpenText Application Quality Management to a new version
- Windows
- SQL database
- Same OpenText Application Quality Management server
- New database server
- New Site Administration schema

Installation Step	Instructions
Prerequisites	• "Prerequisites: Windows Operating Systems" on page 36 • "Prerequisites: Microsoft SQL Database Servers" on page 54 • "Prerequisites: General" on page 58 • "Prerequisites: Client-side" on page 60

Installation Step	Instructions
Project Upgrade Prerequisites	• "Back up projects in existing installation" on page 66 • "Verify domains and projects" on page 67 • "Upgrade preparation troubleshooting" on page 190 • "Repair domains and projects" on page 67 • "Restore backed up projects and repositories" on page 68
Installation	"Install on Microsoft Windows systems" on page 76
Start OpenText Application Quality Management	"Starting the system" on page 123
Project Upgrade	"Project upgrade" on page 176
Manage OpenText Application Quality Management	• "Manage the application server" on page 137 • "Customize system files" on page 166
Troubleshoot the Installation	"Troubleshooting the installation" on page 222

Upgrade with same server - Linux

The table below lists the steps for the following scenario:

- Upgrading OpenText Application Quality Management to a new version
- Linux
- Oracle database
- **Same OpenText Application Quality Management server**
- New database server
- New Site Administration schema

Installation Step	Instructions
Prerequisites	• "Prerequisites: Linux Operating Systems" on page 40 • "Prerequisites: Oracle Database Servers" on page 44 • "Prerequisites: General" on page 58 • "Prerequisites: Client-side" on page 60
Project Upgrade Prerequisites	• "Back up projects in existing installation" on page 66 • "Verify domains and projects" on page 67 • "Upgrade preparation troubleshooting" on page 190 • "Repair domains and projects" on page 67 • "Restore backed up projects and repositories" on page 68
Installation	"Install on Linux systems" on page 95
Start OpenText Application Quality Management	"Starting the system" on page 123

Installation Step	Instructions
Project Upgrade	"Project upgrade" on page 176
Manage OpenText Application Quality Management	• "Manage the application server" on page 137 • "Customize system files" on page 166
Troubleshoot the Installation	"Troubleshooting the installation" on page 222

Upgrade with same database server

This section details the steps for upgrading on Windows and Linux with the same database server.

Upgrade with same database server - Windows

The table below lists the steps for the following scenario:

- Upgrading OpenText Application Quality Management to a new version
- Windows
- SQL database
- New OpenText Application Quality Management server
- Same database server
- New Site Administration schema

Installation Step	Instructions
Prerequisites	• "Prerequisites: Windows Operating Systems" on page 36 • "Prerequisites: Microsoft SQL Database Servers" on page 54 • "Prerequisites: General" on page 58 • "Prerequisites: Client-side" on page 60
Project Upgrade Prerequisites	• "Back up projects in existing installation" on page 66 • "Verify domains and projects" on page 67 • "Upgrade preparation troubleshooting" on page 190 • "Repair domains and projects" on page 67 • "Restore backed up projects and repositories" on page 68
Installation	"Install on Microsoft Windows systems" on page 76

Installation Step	Instructions
Start OpenText Application Quality Management	"Starting the system" on page 123
Project Upgrade	"Project upgrade" on page 176
Manage OpenText Application Quality Management	• "Manage the application server" on page 137 • "Customize system files" on page 166
Troubleshoot the Installation	"Troubleshooting the installation" on page 222

Upgrade with same database server - Linux

The table below lists the steps for the following scenario:

- Upgrading OpenText Application Quality Management to a new version
- Linux
- Oracle database
- New OpenText Application Quality Management server
- Same database server
- New Site Administration schema

Installation Step	Instructions
Prerequisites	• "Prerequisites: Linux Operating Systems" on page 40 • "Prerequisites: Oracle Database Servers" on page 44 • "Prerequisites: General" on page 58 • "Prerequisites: Client-side" on page 60

Installation Step	Instructions
Project Upgrade Prerequisites	• "Back up projects in existing installation" on page 66 • "Verify domains and projects" on page 67 • "Upgrade preparation troubleshooting" on page 190 • "Repair domains and projects" on page 67 • "Restore backed up projects and repositories" on page 68
Installation	"Install on Linux systems" on page 95
Start OpenText Application Quality Management	"Starting the system" on page 123
Project Upgrade	"Project upgrade" on page 176
Manage OpenText Application Quality Management	• "Manage the application server" on page 137 • "Customize system files" on page 166
Troubleshoot the Installation	"Troubleshooting the installation" on page 222

Patch installation

This section provides general instructions for installing and uninstalling patches.

> **Note:** Before installing a patch, review "Installation considerations: Linux" on page 96or "Installation Considerations: Windows" on page 76 for important installation information.

For specific instructions for the patch that you are installing, refer to the *Release Notes*.

This section includes:

Pre-installation checks and considerations

Verify that the patch that you are installing is compatible with your version of OpenText Application Quality Management. You can verify the installed version by going to the **versions.xml** file located under the following:

OS	Path
Windows	**{Installdir}\conf**
Linux	**/var/opt/ALM/conf**

Refer to the patch *Release Notes* for prerequisite and compatibility information.

Full or incremental patch installation

Patch installation provides two packages:

- **Full installation package**

  This package does not require any existing install base and can be used independently.

- **Incremental installation package**

  > **Note:** This package is available for English installation only.

  It is a smaller installer that only contains the differences from your existing 25.1 installation. This package requires that you already installed one of the following:

  - 25.1 GA
  - An earlier patch of 25.1 that is installed also using the incremental installation package.

See the patch release notes for a detailed solution based on your current version.

System Requirements

Verify that your server machine meets the system configurations.

> **Note:** For the most up-to-date supported environments, see the Support Matrix.

Required Permissions - Windows

Verify that you have the required permissions to install on a server machine.

To install a patch on a Windows operating system:

- You must be logged on as a local or domain user with administrator permissions. Your user name cannot include a pound sign (**#**) or accented characters (such as, **ä**, **ç**, **ñ**).

> **Note:** The patch installation must be performed by the same user who performed the full OpenText Application Quality Management installation.

- You must have the following file system and registry key permissions:
  - Full read permissions to all the files and directories under the directory in which OpenText Application Quality Management is installed. The default location for installation files is **C:\Program Files\Micro Focus\ALM**. The patch automatically identifies the correct installation directory path on your server machine. Do not change this path.
  - Full read, write, and execute permissions to the directory on which OpenText Application Quality Management is deployed. The patch automatically identifies the deployment directory that was specified during the initial installation.
  - Full read and write permissions to the repository directory which contains the **sa** and **qc** directories. The repository path is specified by the user during the first installation. The patch automatically identifies the correct repository path on your server machine.
  - Full read permissions to the system root (**%systemroot%**) directory.
  - Full read and write permissions to the installation and configuration log files directory. Installation and configuration log files are written to **C:\ProgramData\Micro Focus\ALM\log**.
  - Full read and write permissions to all the keys under **HKEY_LOCAL_MACHINE\SOFTWARE**.

> **Tip:** The **ProgramData** folder is hidden by default. Files and folders must be visible to view permissions. Show the hidden files by performing the relevant steps for your operating system.

Required Permissions - Linux

To install a patch on a Linux operating system:

- If the repository is located on a remote machine, the application server user account must have network access to the remote repository.
- Your user name cannot include a pound sign (**#**) or accented characters (such as, **ä**, **ç**, **ñ**).

> **Note:** The patch installation must be performed by the same user who performed the full installation.

- You must have the following file system permissions:
  - Full read, write, and execute permissions for all the files and directories under the directory on which OpenText Application Quality Management is installed. The patch automatically identifies the installation path. The installation files are used for configuring the server. By default, the installation files are written to: **/root/ALM**.
  - Full read, write, and execute permissions to the directory on which OpenText Application Quality Management is deployed. The patch automatically identifies the deployment directory specified by the user during the initial installation.
  - Full read, write, and execute permissions to the repository directory which contains the **sa** and **qc** directories. The patch automatically identifies the repository path specified by the user during the initial installation.
  - Full read, write, and execute permissions to the installation and configuration log files directory. Installation and configuration log files are written to: **/var/opt/ALM/log**.
  - Full read, write, and execute permissions to the file delivery logs. The log files are written to: **/var/log**.

- If the file repository is located on a remote machine:
  - On the file server machine, share the file repository directory so that the user running the installation is the owner of the files.
  - **Clustering.** On the machine, or on each cluster node, create a mount directory that points to the file repository directory.

Clustering Configuration

When deploying OpenText Application Quality Management over a cluster, you must install the patch on each of the cluster nodes.

Install the same version of the patch on all nodes, and insert the same repository and database details that you used on the first node.

You must use the same confidential data passphrase on all nodes.

It is important that you enter the repository path using the exact same characters on all nodes. For example, you cannot have the path on the first server node defined as **C:\alm\repository** and on additional nodes defined as **\\server1\alm\repository**. Rather the **\\server1\alm\repository** path must appear on every node.

Install the patch

This section describes how to install patches.

Before installing the patch

1. To prevent loss of files that were added or changed as a result of hot fixes or customization:
   - All files, except for files with a **.class** extension, that were added or changed under the **<Deployment folder>\webapps\qcbin** folder should be copied to the **<Deployment folder>\application\qcbin.war**

folder, including the folder tree hierarchy.

> **Note:** Do not copy over **.class** files from the **qcbin** folder as these files use a different codebase from the patch.

- Any file added or changed under the **<ALM File repository folder>\sa** folder should be copied to the **<ALM File repository folder>\customerData** folder, including the folder tree hierarchy.

After installing the patch and updating the deployment with the changes, the deployment process copies your files back to the **qcbin** and the **sa** folders.

> **Note:** If user avatars are lost after a server upgrade, see this KB article.

2. Make sure that all users are logged out. You can check active connections from Site Administration, in the **Site Connections** tab.
3. Check the *Release Notes* for the patch to see if it contains changes to project database schemas. If so:
   a. **Back up all projects.**
   b. Set project update priorities (optional).
4. Stop the ALM server.

OS	Steps
Windows	In the system tray, right-click the OpenText Application Quality Management icon and choose **Stop Application Lifecycle Management**. Close the tray icon utility by right-clicking the icon and selecting **Exit** There may be multiple system tray icon processes running on the server machine. After stopping the server, ensure that all system tray icon processes are terminated before installation. System tray processes can also be terminated in Windows Task Manager.
Linux	Navigate to the **<Deployment path>/wrapper** directory, and run the following command: **HPALM stop**.

Caution: If the patch includes an automatic upgrade, be aware that the upgraded site administration schema refers to the projects in production.

Note: Before the patch installation (either full or incremental), you do not need to deactivate existing projects.

Installing the patch

There is no need to uninstall any patch before installing a new patch.

Install the patch by performing the following steps on your server machine.

OS	
Windows	Run the ALM_Installer EXE file. Alternatively you can install the patch from the command line. The installation structure is mandatory for proper execution of the OpenText Application Quality Management EXE installer. The directory structure must be kept as is.
Linux	In the command prompt, type: **./ALM_installer.bin**.

Follow the installation and deployment instructions.

Patch installation automatically identifies the installation, deployment, and repository paths from the properties file that was created during the first installation. The file is saved in the following path

OS	Path
Windows	**C:\ProgramData\Micro Focus\ALM\conf\qcConfigFile.properties**
Linux	**/var/opt/ALM/conf/qcConfigFile.properties**

If the installation fails, you receive an error message with the cause of the failure and the path to the log file.

After the patch is installed, the next time users log in, new files are downloaded and installed on the client machines. If file downloads are prohibited through your browser, you can install these files through the OpenText Application Quality Management Client MSI Generator add-in, available on Marketplace.

Uninstalling the Patch

For instructions on uninstalling a patch, see "Uninstall" on page 173.

Installation prerequisites

This section covers prerequisites for installation.

This section includes:

Pre-Installation Checklist

Review and verify the following checklist before installing OpenText Application Quality Management. This checklist outlines the information that

you must supply during the installation process. For detailed prerequisite information, see the chapters in this part that are relevant to your installation.

Check	Information Required
Breaking changes	Check the changes you must know before you install or upgrade. For details, see Breaking changes in Install.
Installation Machine	• Operating system version • CPU type • Free disk space • Free memory **Note:** For the most up-to-date supported environments, see http://admhelp.microfocus.com/alm/specs/alm-qc-system-requirements.htm.
Setup Paths	• Installation path • Deployment path **Note:** • You can accept the default paths offered by the Installation and Configuration wizards, or enter alternative paths. • The installation path must not include folders with accented characters (for example, ä, ç, ñ). • The installation path and the deployment path cannot contain non-English characters. • You must have full permissions on the installation and deployment directories.
License Key	License file
Cluster Description	• Is clustering used? • Cluster hosts

Check	Information Required
Encryption Passphrases	• Communication security passphrase • Confidential data passphrase **Note:** In a cluster, use the same passphrase on all nodes.
Application Server	The port number
Mail Server	• Server type • Server host • Server port
Demo Project	Do you require the Web-based demo application?
Database Server	• Database type • Database version • Database server name • Database administrator user name • Database administrator user password • Database port • Oracle service name (Oracle only) • Default tablespace (Oracle only) • Temp tablespace (Oracle only)
Site Administration	• Site administrator user name • Site administrator password

Check	Information Required
Existing OpenText Application Quality Management /Quality Center Installation	If there is an existing Site Administration schema, provide the following information for the existing version: • OpenText Application Quality Management/Quality Center version • OpenText Application Quality Management/Quality Center host • Confidential data passphrase • Database server name • Database administrator user name • Database administrator password • Site Administration database schema name • Site Administration database schema password • Repository folder location • Site administrator user name • Site administrator password
Repository	Repository folder location
Java (JDK /JRE)	Install Java on the ALM server. For details, see "Prerequisites: General" on page 58. **Note:** When working in a cluster environment, it is highly recommended to install the same version of JDK/JRE on each node.

Prerequisites: Windows Operating Systems

This section provides an overview of the prerequisites for installing OpenText Application Quality Management on Windows-based operating systems.

This section includes:

System Configurations: Windows

Verify that your server machine meets the OpenText Application Quality Management system configurations.

> **Note:** For the most up-to-date supported environments, see Support Matrix.

OpenText Application Quality Management can be deployed on a VMware ESX/ESXi server according to the VMWare guest operating system compatibility matrix.

Required Permissions: Windows

Verify that you have the required permissions to install OpenText Application Quality Management on a server machine.

> **Tip:** Some permissions require access to the **ProgramData** folder. This folder is hidden by default. To show hidden files and folders, perform the relevant steps for your operating system.

- If you are upgrading from a previous version with a remote repository, the application server user account must have network access to the remote repository. For details, contact your network administrator.
- You must be logged on as a local or domain user with administrator permissions. Your user name cannot include a pound sign (**#**) or accented characters (such as, **ä**, **ç**, **ñ**).

  > **Note:** All related installation operations for the same version, such as patch installations or uninstalling OpenText Application Quality Management, must be performed by the same user.

- You must disable User Account Control (UAC) during the installation and configuration.

  > **Note:** In Windows 8, UAC cannot be completely disabled. Instead, use the **Run as Administrator** option during installation and configuration.

- The Distributed Link Tracking Client service must be stopped during the installation and configuration.
- We recommend disabling anti-virus software during the installation and configuration.
- You must have the following file system and registry key permissions:
  - Full read permissions to all the files and directories under the directory in which OpenText Application Quality Management is installed. The installation directory path is specified by the user during installation. By default, the installation files are written to: **C:\Program Files\Micro Focus\ALM**.
  - Full read, write, and execute permissions to the directory on which OpenText Application Quality Management is deployed. The deployment directory is specified by the user during installation.

    > **Note:** Due to a Windows limitation, the deployment directory cannot be on a mapped drive.

  - Full read and write permissions to the repository directory, which contains the **sa** and **qc** directories. The repository path is specified by the user during installation. By default, it is located under the deployment directory.

    > **Note:** Due to a Windows limitation, the repository path cannot be on a mapped drive.

  - Full read permissions to the system root (**%systemroot%**) directory. If you do not have these permissions, you can still install OpenText Application Quality Management, but you cannot install any patches.

- Full read and write permissions to the installation and configuration log files directory. Installation and configuration log files are written to **C:\ProgramData\Micro Focus\ALM\log**.
- Full read and write permissions to all the keys under **HKEY_LOCAL_MACHINE\SOFTWARE\Mercury Interactive**.

Clustering: Windows

Check with your system administrator whether you are installing OpenText Application Quality Management on a single node or as a cluster.

If you are installing on cluster nodes, verify which machine to use as the first node to start the installation and the number of machines you should use. This depends on the number of users and availability considerations.

When installing on additional nodes:

- **OpenText Application Quality Management version.** You must install the same version of OpenText Application Quality Management on all nodes.
- **Operating System.** You must install the same version of the operating system, including all patches, updates, or hot fixes, on all nodes.
- **Site Administration schema.** All nodes must point to the Site Administration schema.
- **Database details.** Configure all nodes with the same database information.
- **Confidential Data Passphrase.** You must use the same Confidential Data Passphrase on all nodes.
- **Repository path.** All nodes must point to the repository path that is defined on the first node. It is important that you enter the repository path using the exact same characters on all nodes. For example, you cannot have the path on the first server node defined as **c:\alm\repository** and on additional nodes defined as **\\server1\c$\alm\repository**—the **\\server1\c$\alm\repository** path must appear on every node.

- **Java Installation.** It is highly recommended to install the same version of JDK/JRE on each node.

Repository Path: Windows

The location of the repository directory is specified by the user during installation. You must have full control permissions to the repository path as described in "Required Permissions: Windows" on page 37.

> **Note:** Due to a Windows limitation, the repository path cannot be on a mapped drive.

Prerequisites: Linux Operating Systems

This section provides an overview of the prerequisites for installing OpenText Application Quality Management on a Linux operating system.

This section includes:

System Configurations: Linux

Verify that your server machine meets the OpenText Application Quality Management system configurations.

> **Note:** For the most up-to-date supported environments, see Support Matrix.

Consider the following for implementing OpenText Application Quality Management configurations:

- Verify that you have a supported kernel by running uname **-a**.
- OpenText Application Quality Management can be deployed on a VMware

ESX/ESXi server according to the VMWare guest operating system compatibility matrix.

Required Permissions: Linux

The following permissions are required:

- Verify that you have the required permissions to install OpenText Application Quality Management on a server machine.
- If you are upgrading from a previous version with a remote repository, the application server user account must have network access to the remote repository. For details. contact your network administrator.
- Your user name cannot include a pound sign (**#**) or accented characters (such as, **ä**, **ç**, **ñ**).

> **Note:** All related installation operations for the same version, such as patch installations or uninstalling OpenText Application Quality Management, must be performed by the same user.

- To install ALM, you must have the following file system permissions:
  - Full read, write, and execute permissions for all the files and directories under the directory on which OpenText Application Quality Management is installed. The installation files are used for configuring the server. By default, the installation files are written to: **/root/ALM**.
  - Full read, write, and execute permissions to the directory on which OpenText Application Quality Management is deployed. The deployment directory is specified by the user during installation.
  - Full read, write, and execute permissions to the repository directory, which contains the **sa** and **qc** directories. The repository path is specified by the user during installation. By default, it is located under the deployment directory.

- Full read, write, and execute permissions to the installation and configuration log files directory. Installation and configuration log files are written to **/var/opt/ALM/log**.
- Full read, write, and execute permissions to the file delivery logs. The log files are written to: **/var/log**.
- If the file repository is located on a remote machine:
  - On the file server machine, share the file repository directory so that the user running the installation is the owner of the files.
  - On the ALM machine, or on each cluster node, create a mount directory that points to the file repository directory.

Minimum Disk Space Requirements

The following partitions have minimum disk space requirements:

- **Installation path (default is /root/ALM).** Requires at least enough free space to accommodate the size of OpenText Application Quality Management after it has been installed. The approximate size of an installation is 1.2GB, though the exact amount of space may vary from installation to installation.
- **Deployment path.** Requires at least enough free space equal to the space on the installation DVD, approximately 800MB. A copy of the installation is stored in this partition.
- **/tmp.** Requires a large amount of free space. The exact amount cannot be specified as this partition is also consumed by the operating system. It is advisable that the amount of free space is equal in size to OpenText Application Quality Management after it has been installed, which is approximately 1.2GB.

Also, the User Process Resource Limits must be set to 4096. Edit **/etc/profile** and add the following line at the end of the file:

```
ulimit -n 4096
```

Clustering: Linux

Check with your system administrator whether you are installing OpenText Application Quality Management on a single node or as a cluster.

If you are installing OpenText Application Quality Management on cluster nodes, verify which machine to use as the first node to start the installation and the number of machines you should use. This depends on the number of users and availability considerations.

When installing on additional nodes:

- **OpenText Application Quality Management version.** You must install the same version of on all nodes.
- **Operating System.** You must install the same version of the operating system, including all patches, updates, or hot fixes, on all nodes.
- **Site Administration schema.** All nodes must point to the Site Administration schema.
- **Database details.** All nodes must be configured with the same database information.
- **Confidential Data Passphrase.** You must use the same Confidential Data Passphrase on all nodes.
- **Repository path.** You must mount the file system repository before you start the installation process. The mount should not use any cache mechanisms. For details, contact your network administrator.

  All nodes must mount the shared file server with the same mount name. For example, if the file server is **some.server.org**, and it is mounted on **/mnt/some_server** on the first node, it should be mounted with **/mnt/some_server** on all nodes.
- **Java Installation.** It is highly recommended to install the same version of JDK/JRE on each node.

Repository Path: Linux

The location of the repository directory is specified by the user during installation. You must have full control permissions to the repository path as described in "Required Permissions: Linux" on page 41.

Prerequisites: Oracle Database Servers

This section provides an overview of the prerequisites for connecting OpenText Application Quality Management to an Oracle database server.

This section includes:

Connecting to an Oracle Database Server

Verify the following:

Database type and version	Verify that OpenText Application Quality Management supports your database type and version. **Note:** For the most up-to-date supported environments, see the Support Matrix.
Database server name	Verify the name of the database server.

Database user permissions	Verify that you have the database permissions required to install OpenText Application Quality Management on the Oracle database server. For a list of required permissions, see "User Permissions for Connecting to an Oracle Database Server" on the next page.
Site Administration database schema	To install on an existing Site Administration database schema (second node or upgrade), you must have: • The existing database schema name and the database administrator permissions required to connect to the database server. • Full read/write permissions on the existing repository. • OpenText Application Quality Management must have access to the previous Site Administration schema repository path. • Full read/write permissions for the OpenText Application Quality Management user to the previous schema repository path. • The Confidential Data Passphrase that was used to create the existing schema. For schema name and password considerations, see "Site Administration Database Schema Considerations: Oracle" on page 51.

Database tablespace name and size	• Verify the name of the database server, and check the connection to the database server. Ping the database server machine name to test DNS resolution. • Verify you have the tablespace names (default and temporary) and the minimum tablespace sizes for storing the Site Administration database schema. • Verify that the tablespace is not locked.
Database Column Length Semantics	For Unicode databases, ensure that column length (NLS_LENGTH_SEMANTICS) is defined according to characters (CHAR), and not according to bytes (BYTE, the default option).

See also:

- "User Permissions for Connecting to an Oracle Database Server" below
- "Database Administrative User Privileges" on page 48
- "Project User Privileges" on page 50
- "Upgrade with new schema" on page 12

User Permissions for Connecting to an Oracle Database Server

To connect to an Oracle database server, the installing database user must have sufficient permissions to perform certain administrative tasks in Oracle. These tasks include creating the project user schema, copying data between projects, and checking that there is sufficient storage in a specific tablespace.

We recommend that your database administrator create an OpenText Application Quality Management database administrative user, for example **qc_admin_db**, with the specific privileges required to install.

Create OpenText Application Quality Management database administrative user	Your database administrator can create an OpenText Application Quality Management database administrative user using a script, see Creating DB administrative user required for ALM installation. This script creates the database administrative user with the recommended grants required on the database. Your database administrator should run the script and create this user on the staging database server. The privileges of the Oracle database user "system" changed after version 12c. If you are working with Oracle Database versions later than 12c, make sure you create an ALM database administrative user by following Creating DB administrative user required for ALM installation and grant the necessary privileges. For details on the required privileges, see "Database Administrative User Privileges" on the next page.
Create OpenText Application Quality Management database administrative user for the optimization of table statistics gathering **(Available for 17.0.1 and later)**	If you want to optimize the project upgrade process, create an OpenText Application Quality Management database administrative user with the specific privileges. This optimizes the table statistics gathering for ALM installation or upgrade. To create an database administrative user for optimized table statistic gathering: 1. Make sure the **UPGRADE_PROJECT_BY_SUPER_USER** site parameter is set to **Y**. 2. Follow the instructions in DB privileges required for the optimization of table statistics gathering.

Database Administrative User Privileges

Following are the privileges required by the OpenText Application Quality Management database administrative user. Additional explanations about these privileges can be found in the notes at the end of the table.

Privilege	Description
CREATE SESSION WITH ADMIN OPTION (1)	OpenText Application Quality Management uses this privilege to connect to the database as the database administrative user.
CREATE USER	Required to create a new project user schema when creating a new project.
DROP USER	When deleting a project, OpenText Application Quality Management attempts to remove the Site Administration database schema from the database server. If there is an insufficient privileges error, OpenText Application Quality Management ignores the error and requests that the user notify the database administrator to delete (drop) the database user schema.
CREATE TABLE WITH ADMIN OPTION (1)	Required for granting this permission to a newly created project user schema.
CREATE VIEW WITH ADMIN OPTION (1)	Required to create views for projects.
CREATE TRIGGER WITH ADMIN OPTION (1)	Required to create triggers for projects. OpenText Application Quality Management uses database triggers to collect change history for specific tables.
CREATE SEQUENCE WITH ADMIN OPTION (1)	Required to create sequences for projects.

Privilege	Description
CREATE PROCEDURE WITH ADMIN OPTION (1)	Required to create stored packages for projects. ALM uses packages to collect change history for specific tables.
CTXAPP ROLE WITH ADMIN OPTION (1)	Enables OpenText Application Quality Management to use the Oracle text searching feature. This role exists only if the Oracle text search component was installed and enabled on the database server.
SELECT ON DBA_FREE_ SPACE (2)	Required to check free space on the database server prior to creating a new Site Administration database schema or a new project.
SELECT ON SYS.DBA_ TABLESPACES (2)	Required to collect a list of tablespaces that exist on the database server prior to creating a new Site Administration database schema or a new project.
SELECT ON SYS.DBA_ USERS (2)	Required to verify the existence of specific database project users. For example, you might want to verify the existence of an Oracle CTXSYS user before creating a new project.
SELECT ON SYS.DBA_ REGISTRY (2)	Required to verify that the text search component is installed on the database server.
SELECT ON SYS.DBA_ROLES (2)	Required to verify that the text search role (CTXAPP) is installed on the database server.
SELECT ANY TABLE WITH ADMIN OPTION (1) **and** **INSERT ANY TABLE**	Required for various administrative operations when upgrading the Site Administration database schema during installation using the copy and upgrade method, and for enhancing performance when copying a project that has the same source and target database server.

Note:

- (1) An ALM database administrative user must have privileges with Admin Option.
- (2) The SELECT ON SYS privileges can be given directly by the table owner, or through a database application role. To avoid giving these privileges each time, you can grant this role to the database administrative user. The recommended name for this role is **QC_SELECT_ON_SYS_OBJECTS**. You should run this script before you run the **qc_admin_db___oracle.sql** script.

Project User Privileges

When creating a new project, a project user schema is created. This user schema hosts all the tables that are used by the project for storing and retrieving data. Following are the required privileges for a project user schema:

Project User Schema Privilege	Description
QUOTA UNLIMITED ON <default tablespace>	Required for creating database objects that are owned by the project user schema. This privilege allows users to create tables in the default tablespace. It replaces the **UNLIMITED TABLESPACE** system privilege that gave users system privileges to create tables in any tablespace, including the **SYSTEM** tablespace.
CREATE SESSION	This privilege is used to connect to the database user schema to perform required operations. For example creating database objects such as tables, and using them to insert, retrieve, and delete data.

Project User Schema Privilege	Description
• **CREATE TABLE** • **CREATE VIEW** • **CREATE TRIGGER** • **CREATE SEQUENCE** • **CREATE PROCEDURE** • **CTXAPP Role**	For a description of these privileges, see "Database Administrative User Privileges" on page 48.

Site Administration Database Schema Considerations: Oracle

Be aware of the following schema name and password considerations:

- The default Site Administration database schema name is **qcsiteadmin_db**. If you want to rename the schema, you can change the name when configuring the installation.

  > **Note:** The Site Administration database schema name can only contain English characters or numbers.

- You can create your own OpenText Application Quality Management user password for accessing the Site Administration database schema.
- If there is an existing Site Administration database schema, you can create a copy of the existing schema and upgrade the copy. This enables you to work with 25.1 and previous versions simultaneously.

Oracle RAC Support

Oracle RAC is a way to enhance Oracle database availability and scalability, allowing it to interact with more than one database instance.

OpenText Application Quality Management RAC support includes:

- Load balancing between Oracle instances.
- Failover between all specified Oracle RAC nodes at initial connection.

OpenText Application Quality Management RAC support does not include:

- TAF (Transparent Application Failover) support. A user failing to complete a request upon an Oracle instance crash is required to perform the activity again with a working Oracle instance.

To enable Oracle RAC support:

1. Verify that a file containing information of Oracle database addresses is saved on your ALM machine. The file is named **tnsnames.ora**. The file should contain information similar to the following examples:
   a. This first example shows an RAC TNS Alias using all cluster nodes in the ADDRESS sub-section and a sample of utilizing the Load balance and Failover features:

Example:

```
OrgRAC =
(DESCRIPTION =
       (ADDRESS_LIST=
              (FAILOVER = on)
              (LOAD_BALANCE = on)
              (ADDRESS= (PROTOCOL = TCP)(HOST = server1)(PORT = 1521))
              (ADDRESS= (PROTOCOL = TCP)(HOST = server2)(PORT = 1521))
              (ADDRESS= (PROTOCOL = TCP)(HOST = server3)(PORT = 1521))
       )
       (CONNECT_DATA=
       (SERVICE_NAME = myrac.yourcompany.com)
       )
)
```

b. This second example shows an RAC TNS Alias using Single Client Access Name (SCAN). This enables Oracle 11gR2 clients to connect to the database with the ability to resolve multiple IP addresses, reflect multiple listeners in the cluster and handle public client connections. For details on working with RAC SCAN, refer to the Oracle documentation.

Example:

```
OrgRAC_Scan =
(DESCRIPTION =
       (ADDRESS_LIST=
              (FAILOVER = on)
              (LOAD_BALANCE = on)
              (ADDRESS= (PROTOCOL = TCP)(HOST = myrac-cluster-scan)(PORT = 1521))
       (CONNECT_DATA=
       (SERVICE_NAME = myrac.yourcompany.com)
       )
)
```

2. Verify that you have the address of the TNS server to which OpenText Application Quality Management should refer, for example, OrgRAC.

Oracle JDBC Driver TNSNAME and Parameters Support

To support Oracle JDBC parameters, you can append the options to the JDBC connection URL in the form of **;<oracle_jdbc_propertie>=<propertie_value>;**.

For example, to use TNSNAME:

```
jdbc:oracle:thin:@OrgRAC;oracle.net.tns_admin=<path of tnsnames folder>
```

Prerequisites: Microsoft SQL Database Servers

This section provides an overview of the prerequisites for connecting to a Microsoft SQL database server.

This section includes:

Connecting to a Microsoft SQL Database Server

Verify the following:

Database type and version	Verify that OpenText Application Quality Management supports your database type and version. **Note:** For the most up-to-date supported environments, see the Support Matrix.
Database server name	Verify the name of the database server.
Database user permissions	Verify that you have the database permissions required to connect to the Microsoft SQL database server (not applicable for Windows Authentication). For a list of required permissions, see "User Permissions for Connecting to a Microsoft SQL Database Server" on the next page.

Site Administration database schema	To install on an existing Site Administration database schema (second node or upgrade), you must have: • The existing database schema name and the database administrator permissions required to connect to the database server. • Full read/write permissions on the existing repository. • OpenText Application Quality Management must have access to the previous Site Administration schema repository path. • Full read/write permissions for the OpenText Application Quality Management user to the previous schema repository path. • The Confidential Data Passphrase that was used to create the existing schema. For schema name and password considerations, see "Site Administration Database Schema Considerations: SQL" on page 58.
Text Search	Verify that the text search component is installed on the server, even if you do not intend to use it.

User Permissions for Connecting to a Microsoft SQL Database Server

To connect to a Microsoft SQL database server, the installing database user must have sufficient permissions to perform certain administrative tasks in SQL.

If you have the SQL **sa** login, you can use it to install OpenText Application Quality Management. If you are unable to use the SQL **sa** login due to security reasons, we recommend that your database administrator create an OpenText Application Quality Management database administrative login, for example **td_db_admin**, with the specific privileges required to install.

The **td_db_admin** login must have the Database Creators role. You must also grant the **td_db_admin** login the Security Administrators role. This allows the **td_db_admin** login to create and add the **td** user with only those privileges required for running OpenText Application Quality Management, and to run the Maintain Project activities, such as Verify, Repair, and Update.

> **Note:** If you are unable to grant the Database Creators and Security Administrators roles, you can grant specific privileges for the database administrative login. For details, see Creating DB administrative user required for ALM installation.

To create a database administrative login on a Microsoft SQL Server:

1. Open the **SQL Server Management Studio**.
2. In the **Object Explorer** pane, under the database server, expand the **Security** folder.
3. Right-click the **Logins** folder, and select **New Login**.
4. Type **td_db_admin** as the login name, and select the authentication type (enter password if necessary).
5. Click the **Server Roles** tab, and select the **dbcreator** and **securityadmin** options.
6. Click **OK.**

To test the database administrative login after connecting via this login (SQL Server Authentication):

1. Verify the **select sysdatabases table** permission in the master database:

```
SELECT name FROM sysdatabases where name=<db_name>
```

2. Verify the **create database** permission:

```
CREATE DATABASE <dbName> -- the database name must not
already exist
```

3. Verify the **drop database** permission:

```
DROP DATABASE <database_name> -- the database name must
exist
```

4. Verify the **select syslogins** permission:

```
SELECT COUNT(*) FROM master..syslogins WHERE
name=<dbOwnerName>
```

> **Note:** The **dbOwnerName** must be set to **td**.

To test the database administrative login permissions after connecting via this login (Windows Authentication):

1. Verify the **change database context** permission:

```
USE <dbName>
```

2. Verify the **create database** permission:

```
CREATE DATABASE <dbName> -- the database name must not
already exist
```

3. Verify the select on **syslogins** permission:

```
SELECT COUNT(*) FROM master..syslogins WHERE
name='<dbOwnerName>'
```

4. Verify the select on **sysusers** permission:

```
SELECT COUNT(*) FROM master..sysusers WHERE
name='<dbOwnerName>'
```

Site Administration Database Schema Considerations: SQL

Be aware of the following schema name and password considerations:

- The default Site Administration database schema name is **qcsiteadmin_db**. If you want to rename the schema, you can change the name when configuring the installation.

  > **Note:** The Site Administration database schema name can only contain English characters or numbers.

- You can create your own OpenText Application Quality Management user password for accessing the Site Administration database schema.
- If there is an existing Site Administration database schema, you can create a copy of the existing schema and upgrade the copy. This enables you to work with 25.1 and previous versions simultaneously.

Prerequisites: General

This topic provides an overview of various prerequisites for installing OpenText Application Quality Management.

License Activation

To activate your license go to the Software Licenses and Downloads Portal using one of the following links:

https://sld.microfocus.com/

Encryption Passphrases

Verify that you have the confidential data passphrase and communication security passphrase.

- Verify that you have the confidential data passphrase and communication security passphrase that you used to install the primary cluster. You must use the same confidential data passphrase and communication security passphrase on all nodes.
- You must use the same confidential data passphrase and communication security passphrase that were used for the previous installation.

> **Caution: Do not change passphrases during installation or upgrade**
>
> If you use a different confidential data passphrase or communication security passphrase than that used for the previous version, stored information such as API key secrets, SMTP passwords, and database server passwords become invalid and cannot be restored. This results in connection failures to all ALM projects and the corresponding systems.

Mail Server Information

A mail server enables OpenText Application Quality Management users to send emails to other users in a project. You select which server to use as part of the installation configuration process.

Before installing, decide which mail server to use. Ask your system administrator for assistance. If you are using an SMTP Server, check that you have the SMTP Server name and port. The installer checks that the specified mail server name and port are valid and that the mail server is running.

Java Installation

Java Development Kit (JDK) or Java Runtime Environment (JRE) is required before installing OpenText Application Quality Management.

> **Note:** When working in a cluster environment, it is highly recommended to install the same version of JDK/JRE on each node.

For supported JDK versions, see the Support Matrix.

Conflicting Applications

To work with OpenText Application Quality Management, you may need to disable conflicting applications that are running on the OpenText Application Quality Management machine. For a list of these applications, see this KB article.

Prerequisites: Client-side

This section provides an overview of the prerequisites for working with OpenText Application Quality Management on a client machine. The steps described in this chapter are performed on the client machines, and not on the machine on which OpenText Application Quality Management server is installed.

This section includes:

System Configurations

Verify that client machines meet the system configurations see the Support Matrix.

Additional Considerations

The following considerations must also be taken into account:

- If you are integrating with other OpenText testing tools, you must modify the DCOM permissions on your client machine. For details, see this KB article.

  ALM Edition: Modifying DCOM permissions is not required for running Functional test sets (server-side test execution).
- You can work with the client using a remote desktop.
- For customers using remote or mass distribution mechanisms, client components can be deployed locally on client machines by running a self-extracting **msi** file. You build the **msi** file by running the ALM Client MSI Generator, available from Marketplace.

Permissions Required to Download Client Components

To enable OpenText Application Quality Management to work with OpenText testing tools as well as various other integrations and third-party tools, you need to log in to the client machine with administrator privileges. These privileges are required to install the ALM Client Registration add-in, which you use to register client components and Site Administration client components on your client machine.

File System Permissions

You must have the following file system permissions:

- Full read and write permissions on the HP\ALM-Client deployment folder. This is located at %ALLUSERSPROFILE%.
- Full read and write permissions to the Temp (%TEMP% or %TMP%) directory. The installer program writes installation and log files to this directory. This is generally located at C:\Users\<username>\AppData\Local\Temp.

Windows - Enabling User Account Control (UAC)

If you enable UAC on a Microsoft Windows 7, 2008R2, or 2012 operating system, be aware of the following considerations:

- To register client components, you must run Internet Explorer as the administrator.
- To register client components on a shared location of a client machine, you must run Internet Explorer as the administrator.
- To install and run ALM Client MSI Generator, and to run ALM client MSI files, you must log in with administrator permissions.
- Administrator permissions are required to run the OpenText Application Quality Management Tray Icon.

Pre-Installation project upgrade steps

This section covers pre-installation project upgrade steps.

This section includes:

Upgrade versions

The following table describes the latest versions to which you can directly upgrade projects from previous versions.

From versions	Latest version to support direct upgrade
11.0	12.2
11.5x	12.5
12.0	15.0
12.2	15.5
12.5x	16.0.x
12.6x	17.0.x
15.0.x	24.1
15.5.x	25.1.x
16.x.x	26.1
17.x.x	26.1
24.1.x	26.1
25.1.x	26.1

Caution: Before performing any upgrade, the current repository must be moved to the correct location for the new version.

Suggested system configuration

The system includes the following main components: The OpenText Application Quality Managementserver, the database server, and the project repository. For details regarding the function of each component within the system, see " Technology and Architecture" on page 3.

When planning your installation and upgrade strategy, decide whether to install the new OpenText Application Quality Management system on new system components, or to reuse components from the existing system.

It is strongly recommended that you not use any of the existing components as part of the new system.

- **Application server.** To install the new version of the OpenText Application Quality Management server on the same machine where the existing server is installed, first reformat or reinstall the machine's operating system. You can also uninstall the old version. For more details on uninstalling, see "Uninstall" on page 173.
- **Database server.** Install an updated version of the database server on a separate machine, or create a new instance of the existing server on the machine on which it is currently installed.
- **Project Repository.** Create a copy of the existing repository to be used by the new system.

Advantages

Following this best practice produces two functioning systems:

- The original system that can open and work with existing projects.
- The new system to which existing projects will be upgraded.

Each system is totally separate, and any problem encountered in one does not impact the other.

This best practice has the distinct advantage of enabling you to incrementally upgrade your projects. Since there are two functioning systems, there is no need to deactivate all projects at once. You can deactivate projects individually in the old system, back them up, and then reactivate them in the new system, upgrading them one-by-one. Without two functioning systems, all projects would remain inactive until their upgrades are complete, a significant amount of project downtime.

> **Note:** Before beginning the upgrade process you must back up the database server and the project repository. Continuing to work in the old system after backing up causes the backup to be out of date.

The following are two examples of critical problems that may arise when you do not follow the suggested upgrade approach:

- **Unnecessary project downtime.** If a project becomes corrupted before you complete its upgrade, there will be no option but to retrieve a backup copy of it. Depending on organizational policy this process may take a few days, meaning that the project is not available at all for this amount of time.

  If the original system is functioning however, you can go back to a working version of the project immediately and not be dependent on waiting for the backup to arrive, thus avoiding unnecessary project downtime.
- **Damaged project repository.** If you install the new version of the server on the same machine, you must first uninstall the existing server. It is possible that you may subsequently discover a problem with the project repository that requires the original server to repair it.

  Your only course of action is to:

  a. Uninstall the new version.

  b. Reinstall the old version.

  c. Fix the project repository.

d. Uninstall the old version.

e. Reinstall the new version.

Back up projects in existing installation

Back up all your projects in the existing installation. Projects should be backed up before running the verify and repair tools.

When you run the repair or upgrade process, OpenText Application Quality Management performs changes on your projects to align them with the specifications for the current version. You must back up your projects before you start to repair or upgrade them.

We strongly recommend that you deactivate projects before backing them up. If you must back up while your project is still active, you must back up the database before the file system. We also recommend backing up the file system as soon as possible after backing up the database. To back up and restore data from active projects, see this KB article.

Note:

- The repair process makes changes to the project database schema only. Before running the repair process, you should back up the project database schema on the database server, and you should back up the project data in the file system.
- Before you run the upgrade process, perform a full backup of your projects that includes the project database schema and the project repository.
- **Version Control:** Version control enabled projects cannot be backed up while there are checked out entities. All entities must be checked in to the corresponding version of OpenText Application Quality Management. To determine if there are checked out entities, see this KB article.

To back up the project database schema on the database server:

- **Microsoft SQL database.** To back up the project database schema on the database server, see this KB article.
- **Oracle database.** To back up the project database schema on the database server, see this KB article.

Verify domains and projects

Verify all projects in the existing installation.

The verify and repair process checks that the project schema structure and data integrity are correct for the existing version. It is important to verify this before proceeding with the new installation, since the projects on the old server should be aligned prior to upgrade.

You can run the verify tool per individual project, or on the domain level to verify all projects in the domain.

Repair domains and projects

The repair process fixes most data and schema issues found by the verification process. If the verification process finds problems that can cause data loss, the repair process does not fix these automatically. You need to repair these problems manually. To find out whether a particular issue is handled automatically or manually, refer to the verification report.

By default, the repair process runs in non-silent mode. When running the process in non-silent mode, OpenText Application Quality Management may pause and prompt you for input when an error occurs. Instead, you can choose to run the process in silent mode. When an error occurs, the process is aborted without prompting you for input.

For detailed information on the problems fixed by the repair process, and help with repairing problems that cannot be fixed by OpenText Application Quality Management, see "Upgrade preparation troubleshooting" on page 190.

Restore backed up projects and repositories

If the repair or upgrade process fails, you must restore the backed up projects before trying the process again. You can restore projects that were backed up on an Oracle or Microsoft SQL database server, and you can restore project repositories that were backed up in the file system. A project you restore can be used only in the version from which it was backed up. Before restoring the backed up project, you must remove the project from Site Administration.

If you were working with OpenText Enterprise Performance Engineering 11.00 or later, before restoring a project that has the ALM Lab Extension enabled, you must first restore **LAB_PROJECT**, and then any template projects. For details, see Manage LAB_PROJECT

Verify projects again

Before proceeding, run the verification tool again to make sure that all problems have been fixed.

Copy Site Administration database schema to the new database server

To upgrade a copy of the Site Administration database schema on a new database server machine, you must copy the schema from the database server that was used in the previous system to the database server that will be used in the new system.

You perform this step before installing 25.1 because the schema upgrade option is defined as part of the installation configuration.

Perform the required steps for backing up, removing, and restoring databases for your database type. For assistance contact your database administrator.

> **Note:** The database user must have the same permissions as the user installing OpenText Application Quality Management.

When copying and upgrading the Site Administration database schema, ensure that the existing project refers to the production project database and shared repository, if applicable. When using a staging or side by side upgrade prior to starting the server update, update the following columns in the PROJECTS table in the Site Administration database schema to their new values:

- PHYSICAL_DIRECTORY
- DBSERVER_NAME
- DB_CONNSTR_FORMAT
- DB_USER_PASS

Upgrade the Site Administration database schema

When installing 25.1, you can choose to create a new Site Administration schema on the database server, or you can upgrade a copy of the existing schema. This section discusses considerations, guidelines, and prerequisites for upgrading a copy of the existing schema.

This section includes:

Schema Upgrade Guidelines

Upgrading a copy of the existing schema is a useful option if you are installing 25.1 on a new server machine. Creating a copy of the existing schema and then upgrading the copy enables you to work with new and upgraded projects.

Example:

If your OpenText Application Quality Management 12.00 schema contains a project called **my_project,** by creating a copy of the Site Administration 12.00 schema and then upgrading it to 25.1, the **my_project** project is available in Site Administration in both 12.00 and 25.1.

Oracle database servers: The new database schema is created in the same tablespace as the existing Site Administration database.

When you upgrade a copy of the existing Site Administration database schema, the copy that is created is independent of the existing schema. Any changes subsequently made to the original schema through updates in your previous version are not reflected in the upgraded copy of the Site Administration database schema that 25.1 uses.

Therefore, consider the following guidelines:

Users	After you install 25.1, if you add or delete users or update user details in your previous version, you must make the same changes in 25.1.
Configuration parameters	After you install 25.1, if you modify configuration parameters in your previous version, you must make the same changes in 25.1.
Server node configuration	If you are working with server nodes, in the Servers tab in Site Administration for 25.1, you must reconfigure the settings for the log file and the maximum number of database connections.

Repository path	The repository path in your previous version must be defined as a network path, so that it can be accessed by both the previous installations and by 25.1. Make sure that the project is active on one server but not on both.

Recover a lost confidential data passphrase

The Confidential Data Passphrase encrypts passwords that are used for accessing external systems (databases and LDAP).

When configuring the installation, you must enter the same passphrase that was used in the previous installation. If you do not know the passphrase, perform the following steps.

> **Note:** This procedure can be performed whether you are installing 25.1 on the same machine as the existing installation, or on a new or separate machine, for example, if you are adding a node to a cluster. If you are not sure on which server machine to install 25.1, see"Suggested system configuration" on page 64.

1. On the machine where OpenText Application Quality Management is currently installed, navigate to the **conf** directory:

OS	Location
Windows	**C:\ProgramData\Micro Focus\ALM\conf** By default, the **ProgramData** folder is hidden. To show hidden files and folders, perform the relevant steps for your operating system.
Linux	**/var/opt/ALM/conf**

2. Create a copy of the **qcConfigFile.properties** file

   If you are installing on a new server machine, place the copy on the machine where you plan to run the new installation. Place the file in the same location on the new machine.

   > **Tip:** If the **conf** directory (Windows: **...\ALM\conf**, Linux: **.../ALM/conf**) directory does not exist on the new server machine, manually create it. In such a case, make sure that the new directory has the required permissions to be accessed by the configuration tool.

3. Open the file and delete all information except for the line that starts with **initstring**.
4. Save the copy. If you are installing on a new machine, skip to step 6.
5. If you are upgrading on the same machine as the previous installation:
   a. Uninstall the current version. For information about uninstalling , see "Uninstall" on page 173. Uninstalling does not remove the existing **qcConfigFile.properties** file.
   b. Overwrite the existing **qcConfigFile.properties** file with the version you edited in step 3.
6. When you run the installation, the wizard detects a previous installation and prompts you to accept the current settings. Accept the current settings. When the wizard reaches the Security page the previous Confidential Data Passphrase appears.

Manage schema changes

Changes to the existing Site Administration database schema may cause the upgrade process to fail. Examples of such changes are the deletion of tables or columns, or changes to field types.

If you are sure that the schema has been changed manually, perform the steps below to ensure a successful schema upgrade.

If you are unsure if the schema has been changed, proceed with the installation as normal. If the schema has been changed, the configuration process fails if the changes cannot be handled automatically. It is important that not all schema upgrade failures are the result of the schema changes. Check the error logs very carefully to identify the exact cause of the failure. If it is apparent that the failure was due to changes to the schema, proceed with the steps below. You will have to run the configuration process again.

To prevent the upgrade process from failing, perform one of the following actions:

> **Note:** It is advisable to perform these actions in this order.

1. Manually repair inconsistencies between the old schema and the new schema. For details about manually repairing the old schema, see "Change the database user schema" on page 216.
2. If the change is known and you are sure the upgraded server can work with it, you can create an exception file that instructs the system to ignore these changes during the upgrade process. After creating the exception file, save it in an accessible location on your system. After installing, the Site Administration Database Schema page in the wizard prompts you to add the file to the configuration process. As a result, the changes to the existing schema do not cause the upgrade process to fail.

   To create an exception file:

   a. Copy the **SchemaExceptions.xml** file from the installation directory. By default, the file is located in: **<Installation path>\ALM\data\sa\Admin\MaintenanceData**

   b. Place the copy of the file in an accessible location on your system.

   c. Edit the file and define exceptions. For example:

- 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 index:

```
<IndexMissing>
<object pattern="MY_INDEX" type="extra">
</IndexMissing>
```

- For an extra constraint:

```
<ConstraintMissing>
<object pattern="MY_CONSTRAINT" type="extra">
</ConstraintMissing>
```

- For multiple occurrences of extra elements:

  For example, multiple extra columns:

```
<ColumnMissing>
<object pattern="MY_COLUMN_1" type="extra"/>
<object pattern="MY_COLUMN_2" type="extra"/>
</ColumnMissing>
```

d. Save the **SchemaExceptions.xml** file.

3. If you cannot manually repair the inconsistencies, or create an exception file, create a new schema and then migrate the projects to the new schema.

   If OpenText Application Quality Management is already installed on the server machine, you can rerun the Installation Wizard.

   a. In the Site Administration Database Schema page, select **Create a New Schema**.

   b. After the configuration process completes, migrate projects to the new schema using the **Restore Project** option in Site Administration.

Installation and configuration

This section covers installation and configuration.

This section includes:

Install on Microsoft Windows systems

This section describes how to install on Windows operating systems. It also describes how to install silently.

> **Note:** For installation troubleshooting details, see "Troubleshooting the installation" on page 222.

This section includes:

Installation Considerations: Windows

Before installing, consider the following:

Default paths	• **Installation path:** `C:\Program Files\Micro Focus\ALM` • **Server deployment path:** `C:\ProgramData\Micro Focus\ALM` • **Repository path:** `C:\ProgramData\Micro Focus\ALM\repository`
Paths and files created automatically by the ALM	• `C:\ProgramData\Micro Focus\ALM\conf` • `C:\ProgramData\Micro Focus\ALM\log`

Logs	The locations of the **Site Administration** and **client** log files are subject to your settings. You can verify the locations from Site Administration. The **installation** log file is located in the ALM server installation folder. The **deployment** log file is located in `C:\ProgramData\Micro Focus\ALM\log`.

Installation scenarios	• **Upgrading from 15.5.x or earlier to 25.1.** When upgrading a copy of an existing Site Administration database schema, consider the following:
	  • If you are **using the existing settings as default**, the default deployment path will be the same as the path used in the previous installation. This path can be changed.
	  • If you are **not using the existing settings as default**, the default deployment path will be `C:\ProgramData\Micro Focus\ALM`. This path can be changed.
	
	Note: The repository path of the upgraded projects will be the same as the path used in the previous installation.
	
	After upgrading, the newly created projects will use the repository path that was defined during the current installation.
	
	If you want to use the same repository path as it was before (default: `C:\ProgramData\HP\ALM\repository`), make sure to set it correctly during installation.

JAVA path used	• When you start the installer, the Java you are using is the one specified by `JAVA_HOME`. This variable is set when installing Java. For details, see "Prerequisites: General" on page 58. • During the installation, the path you specified for the JDK or JRE folder is written to the `MICRO_FOCUS_JAVA_PATH` variable. It indicates the Java path used by OpenText Application Quality Management. For details, see "Install on Windows" below. To check the value of this variable, open Advanced system settings, and in the system variables table, find `MICRO_FOCUS_JAVA_PATH`. For details, see the Microsoft documentation.

Install on Windows

Before installing, consider the following:

- Verify that you meet the various installation prerequisites. For prerequisite information, see the relevant chapters in "Installation prerequisites" on page 33.
- If you are planning to upgrade a copy of the existing Site Administration schema, the database server of the existing Site Administration schema and the database server of the existing Lab Project must be supported. If these database servers are not supported, you can disable the validation check. For details, refer to "Disabling validation checks for the installation wizard" on page 222.

  Note: For the most up-to-date supported environments, see the Support Matrix.

- If you encounter problems during the installation process, see "Troubleshooting the installation" on page 222 for troubleshooting suggestions.

- If you want to reconfigure OpenText Application Quality Management after the installation and configuration is complete, you must run the installation procedure again.
- If an error occurs during the installation procedure, you must uninstall and restart the installation procedure.
- If an error occurs during the installation procedure and the installation log file is not found, ensure that enough disk space is available for installation and deployment to the selected locations, and that system settings such as the open file resources limit are set to the maximum allowable value.

To install on Windows:

1. Log in to the server machine with the appropriate permissions. For a list of required permissions, see "Required Permissions: Windows" on page 37.
2. If OpenText Application Quality Management is installed on the machine, uninstall it. For information on uninstalling, see "Uninstall" on page 173.

   Cluster environment: Uninstall ALM from all nodes.

3. Make sure the following services are started on the machine:
   a. Secondary Logon
   b. Windows Management Instrumentation
4. Run the **setup.exe**, and click **ALM Platform (Windows OS)**.

   Note:
   - The configuration settings are saved in the **qcConfigFile.properties** file. The file is created in the **C:\ProgramData\Micro Focus\ALM\conf** directory.
   - Also, the **repid.txt** file is created in the **<ALM Repository path>\qc folder**. The file should not be moved from this location.
   - If you are installing OpenText Application Quality Management on a secondary node of a cluster, some of the dialog boxes that are needed only for the primary node are not displayed.

5. The Installation wizard starts, displaying the Welcome page. Click **Next**.
6. The License Agreement page opens.

   Read the license agreement. To accept the terms of the license agreement, select **I accept the license terms**. Click **Next**.
7. In the JDK/JRE Path step, browse to or enter the JDK or JRE folder path. Click **Next**.

   The JDK or JRE folder path you specified in this step is written to the qcConfigFile.properties file and MICRO_FOCUS_JAVA_PATH. It can be different from the value of the JAVA environment variable JAVA_HOME. For details about MICRO_FOCUS_JAVA_PATH and JAVA_HOME, see "Installation Considerations: Windows" on page 76.

   > **Required only if you use the Microsoft SQL Server (Windows Auth.) authentication type:**
   >
   > a. In your JRE/JDK's bin folder, which is specified in JAVA_HOME, back up and remove the old mssql-jdbc_auth*.dll file if any.
   > b. Copy the **mssql-jdbc_auth-8.2.2.x64.dll** file from the installer folder (where you extracted the install.zip file) to your JRE/JDK's bin folder. If there is a jre folder under the JDK folder, copy the file to both the JDK/bin and JDK/jre/bin folders.
   >
   > If the values of MICRO_FOCUS_JAVA_PATH and JAVE_HOME are different, also copy the **mssql-jdbc_auth-8.2.2.x64.dll** file to the bin folder of the JDK or JRE folder specified by MICRO_FOCUS_JAVA_PATH.
8. In the Folder Selection step, browse to or enter the installation path, or accept the default. Click **Next**.
9. If the wizard detects settings from a previous installation, the Current Settings page opens.

   Select **Use default values of existing configuration** to use the current settings as default settings for the current installation. You can make

changes to any of the default settings during the wizard. Select **No** to clear all settings in the Configuration wizard.

Click **Next**

10. The Database Server page opens.
    a. Under **Database Type**, select the database type to be used in your OpenText Application Quality Management system.

Oracle	Uses Oracle authentication
MS-SQL (SQL Auth.)	Authenticates the user to the database using a database user name and password.
MS-SQL (Windows Auth.)	Windows authentication relies on the user being authenticated by the operating system.
MS-SQL (AAD Auth.)	Authenticates the user to the database using an Azure AD account.

> **Note:** When upgrading projects to 25.1, you must use the same type of SQL authentication that you used when that project was originally created.

For details on database requirements, see "Prerequisites: Oracle Database Servers" on page 44 or "Prerequisites: Microsoft SQL Database Servers" on page 54.

    b. Select one of the following options:
    - **Database Parameters.** Select this option to enter database server information using the following fields:

DB host name	Type the database server host name or IP address. For example, **dbsrv01.domain.com**.
DB port number	Type the database server port number, or accept the default port number.

Oracle service name	If you selected Oracle as the database type, type the Oracle service name.

- **Connection String.** Select this option to type a formulated database server connection string.

Oracle RAC database	Select **Connection String**, and enter a connection string, specifying the folder that contains the **tnsnames.ora** file, and the TNS server to which ALM should refer. Use the following example: `jdbc:oracle:thin:@OrgRAC;oracle.net.tns_admin=c:\oracle\NETWORK\ADMIN;` For details on prerequisites for Oracle RAC support, see"Oracle RAC Support" on page 52
Microsoft SQL Server database	If your database requires SSL/TLS access, see "Configure a secure database connection for a new installation" on page 165.

c. **DB admin user name.** Type the name of the user with the administrative permissions required to install on the database server.

d. **DB admin password.** Type the database administrator password.

> **Note: DB admin user name** and **DB admin password** are not applicable for Microsoft SQL Server Windows Authentication.

Click **Next**.

11. The Site Administration Database Schema page opens.

a. In **Select Action**, choose one of the following:

Create a New Schema	Creates a new Site Administration database schema and a new Lab_Project. **Note:** The installation log and the enable_extensions.txt file contain error messages stating "Schema differences were found". These errors can be ignored, they are generated as part of the schema enable extension mechanism and the upgrade mechanism.
Upgrade a copy of the existing schema	Creates a copy of the existing Site Administration database schema, and upgrades the copy. For details, see "Schema Upgrade Guidelines" on page 70. If you select this option, the Schema Exception File option appears. If you have defined an exception file for the upgrade process, click **Browse** and navigate to the location where it was saved before the installation. For details about exception files, see "Manage schema changes" on page 72. When working in a cluster environment, select this option if you have an existing primary node and you want to install OpenText Application Quality Management. **Note:** When you upgrade a copy of the existing Site Administration schema, OpenText Application Quality Management tries to copy LAB_PROJECT to the database server where the original LAB_PROJECT exists. If LAB_PROJECT is successfully copied, the new upgraded Site Administration schema points to the new copy of LAB_PROJECT. If LAB_PROJECT is not copied, a new empty LAB_PROJECT is created in the database server where the new Site Administration database schema is created. For details, see "LAB_PROJECT installation considerations" on page 121

Connect to existing schema / second node	This option can be used in two scenarios: ◦ If you are reinstalling and would like to reconnect to the same Site Administration database schema. ◦ If you have an existing node and you want to install on another node to create a cluster. For details on cluster configuration, see "Clustering: Windows" on page 39. **Note:** This option enables you to connect to a 25.1 Site Administration database schema only. To connect to an earlier version, you must first upgrade the schema. For details, see"Upgrade the Site Administration database schema" on page 69.

b. When creating a new schema, in **Database Name**, enter the name of the database.

c. When connecting to OpenText Application Quality Management on an **Oracle database server**:

   If you are installing on a secondary node or if the Site Administration database already exists, the new Site Administration database schema is created in the same tablespace as the existing schema. Continue with the Security step below.

   Type the following information:

   ◦ **Default Tablespace.** Select a default storage location from the list.

   ◦ **Temporary Tablespace.** Select a temporary storage location from the list.

d. Under **SA Schema Details**, type the following information:

   ◦ **Schema name.** Type a Site Administration database schema name, or accept the default schema name. The Site Administration database schema name can contain English characters or numbers only.

- **Schema password.** Enter the following information, depending on your database type:

Oracle:	The default **tdtdtd** password is created, which you can accept or change.
Microsoft SQL Server (SQL Auth.):	OpenText Application Quality Management uses the **td** user to create the Site Administration database schema. For more details on the **td** user, see "User Permissions for Connecting to a Microsoft SQL Database Server" on page 55. Type a password for the **td** user that complies with your organization's password policy, or keep the default **tdtdtd** password.
Microsoft SQL Server (Windows Auth.):	Not applicable.
Microsoft SQL Server (AAD Auth.)	Enter the name and password of the Site Administration database schema name, or keep the default **tdtdtd** password.

- **New Schema name.** If you selected **Upgrade a copy of the existing schema**, type a name for the upgraded copy of the database schema. The Site Administration database schema name can only contain English characters or numbers.

> **Note:** When upgrading an existing Site Administration database schema to work in 25.1, you must use the same name that you used before the upgrade.

Click **Next**.

12. The License Key page opens.

Note: If you selected **Connect to existing schema / second node** in the previous step, the License Key step is skipped. Continue with the Security step below.

Select one of the following options:

ALM server license key	Browse to or enter the OpenText Application Quality Management license file path.
Use Evaluation Key	If you do not have a license file, select this option for a 30-day trial version. From the drop-down list, select the edition to install for the trial period. **Note:** If you install Quality Center Community Edition, you must assign named licenses to your users. Only then can the users successfully log in to ALM and see the appropriate modules.
License URL Parameters	This option configures the AutoPass License Server (APLS). a. Enter the license server **host** and **port**. b. To secure the communication, select **HTTPS**. Alternatively, you can also configure APLS after the ALM installation. Perform the following steps: a. From the ALM server machine, navigate to `C:\ProgramData\Micro Focus\ALM\repository\sa\Admin\MaintenanceData\conf` b. Edit `clusterSettings.properties` c. Define values for the following fields: AUTOPASS_SERVER_PROTOCOL, AUTOPASS_SERVER_PORT, AUTOPASS_SERVER_NAME. d. Save and restart the ALM server.

Click **Next**.

13. The Security page opens.

    a. Confidential Data Encryption

    Passwords for accessing external systems (databases and LDAP) are stored by OpenText Application Quality Management after encryption. Enter a **Confidential Data Passphrase** that is used to encrypt the information.

Make a note of the passphrase for future support calls. You need the passphrase if you choose to redeploy OpenText Application Quality Management and choose to upgrade a copy of the existing Site Administration Database Schema. The passphrase is also required for the next installation.

Select **Use default value for Passphrase** to use the default Confidential Data Encryption passphrase. By selecting this option, the encrypted information is more vulnerable to unauthorized access.

> **Note:**
>
> - After completing the server configuration wizard, you cannot change the confidential data encryption passphrase.
> - The passphrase is case-sensitive. Also check that there are no empty spaces before or after the passphrase. The passphrase must contain only alphanumeric characters.
> - If you do not have a note of the confidential data passphrase, there is a workaround to recover it. However, you will have to abort the configuration process and then begin again once the workaround is complete. For details, see"Recover a lost confidential data passphrase" on page 71.

b. Communication Security

Communication between OpenText Application Quality Management and other applications is enabled after authentication by a Single Sign-On (SSO) token. Enter a communication security passphrase that OpenText Application Quality Management uses to encrypt the SSO token.

> **Note:**
>
> - The communication security passphrase is stored as the value of the **COMMUNICATION_SECURITY_PASSPHRASE** site configuration parameter.

- The passphrase must contain only alphanumeric characters, and must contain at least 12 characters .

Passphrases considerations

- You must use the same passphrases (both confidential data passphrase and communication security passphrase) that were used for the previous installation.
- If you are planning to migrate, restore, or import extension-enabled projects (such as LoadRunner Enterprise and/or Lab Management enabled projects)onto the server on which the project was originally created, you must use the same passphrases that were defined on the server on the original server.
- If you are installing on a cluster, you must use the same passphrases for all nodes.

Caution: If you use different passphrases than those for the previous version, stored information such as API key secrets, SMTP passwords, and database server passwords become invalid and cannot be restored. This results in connection failures to all ALM projects and the corresponding systems.

14. The Site Administrator User page opens.

    You use the site administrator name and password that you define here to log in to Site Administration for the first time. After installation, you can change the site administrator or add other site administrators. Enter a site administrator user name (maximum length 60 characters) and password, and retype the password to confirm.

    If you are upgrading a copy of the existing Site Administration database schema, by default the same user and credentials are applied to the upgraded schema. To create an additional user, select **Create additional Site Administrator user** (this field appears only when you are upgrading a copy of the existing schema).

> **Note:**
>
> - The user name cannot include the following characters: **\ / : * ? " < > |**
> - The password cannot be longer than 20 characters.
> - It is important that you remember the site administrator user name and password so you can log in to Site Administration.

Click **Next**.

15. The ALM Service page opens.

    Type the **User Name**, **Password**, and **Domain** to be used to run the application server as a service. This enables the service to access your local network.

    If the repository is on a remote machine, or if you are using a Microsoft SQL server with Windows authentication, enter the details of a domain user who has administrative permissions for the SQL server and who is a local administrator.

    Click **Next**.

16. The Repository page opens.

    In the **File repository path** box, click the browse button to choose a repository path, or accept the default path. Make sure to enter a unique, case-sensitive name for the repository folder.

> **Note:**
>
> - Make sure you select a path where you have full read and write permissions.
> - To work with cluster nodes, make sure that all nodes have access to the file repository path and that the path is UNC. All nodes in the cluster must have the same string for the repository path.
> - The length of the file repository path cannot exceed 200 characters.
> - The file repository path cannot reside on the root folder.

- Due to a Windows limitation, the file repository path cannot be on a mapped drive.

Using the **BASE_REPOSITORY_PATH** site configuration parameter, you can create a location for a repository path where new projects will be located. Performing this action, therefore, means there will be two repository paths: the previous path containing older projects, and a second path containing projects created subsequently.

Click **Next**.

17. The Application Settings page opens.
    a. In the **Deployment Path** box:

       Specify the location in which you want to deploy application files. Click the browse button to choose a location, or accept the default location. We recommend that you keep the default.

       Note:
       - The length of the deployment path cannot exceed 200 characters.
       - Due to a Windows limitation, the deployment path cannot be on a mapped drive.

    b. In the **Web Server** box:

       Change or keep the default HTTP port number. The default port is 8080.

       Note: If an error message is displayed that the default port is unavailable, the port may be in use by another application running on the server machine. Either locate the application and stop it, or enter a different port number. To enter a different port number, you must first change the port number on the application server. For details, see . Then proceed with the configuration as normal.

c. Select **Start ALM server once installation completed** to automatically start the server when the installation is successfully completed.

Click **Next**.

18. The Mail Service page opens.

    To enable OpenText Application Quality Management to send emails to users in a project, select a mail protocol. For **SMTP Service**, type the server name and port.

    If you selected **Microsoft IIS SMTP Service**, you must configure the Microsoft IIS SMTP service. For details, see "Configure the IIS Mail Service" on page 95.

    Click **Next**.

    > **Note:** The Mail Server can be configured after installation in Site Administration. For details, refer to the online help.

19. The ALM Client Launcher page opens.

    ALM Client Launcher is a tool that allows you to run an ALM client on any Windows machine without the need of deploying it from an ALM server and without Windows administrator permissions.

    From this page, you can:

    - Click the marketplace link to download ALM Client Launcher and learn more about the tool.

      You can also download ALM Client Launcher after the ALM installation.

    - Check the **Package client files in the server for ALM Client Launcher** option to have client files automatically packaged in the server.

      We recommend you check this option if you want to use ALM Client Launcher. It saves you from manually uploading client files to the server. Users that have downloaded ALM Client Launcher can seamlessly run an ALM client upon the successful ALM installation.

> **Note:** Skip this page if you do not plan to use ALM Client Launcher.

20. The Installation Summary page opens. To change any settings, click **Previous**.

    Understand the breaking changes in this version by clicking the help link and select the **Acknowledge all the breaking changes** checkbox. Click **Next** to continue.

21. The Install Complete page opens.

    If the installation process ends with warnings, check the installation logs for details, and start the server manually. For details see "Checking the installation and configuration log files" on page 227.

22. If you are prompted to restart the machine, you can choose to restart at a later time, but you must restart before you use OpenText Application Quality Management. You must also restart before you install any related files, such as integration add-ins.

23. If you are using an Oracle RAC database, verify that the **ORACLE_RAC_SUPPORT** site configuration parameter is set to **Y**. For details, refer to the online help.

24. The installation is now complete. Proceed to "Starting the system" on page 123.

Install in silent mode on Windows

A silent installation runs the entire setup process in the background without requiring you to navigate through setup screens and input selections. Instead, all configuration parameters are assigned values that you define in a configuration file (**qcConfigFile.properties**). When running an installation in silent mode, no messages are displayed. Instead, you can view installation information in the log file, including information on whether the installation was successful. The installation log file can be found under the **<installation folder>\log** directory. The deployment and configuration log file can be found in the following path **C:\ProgramData\Micro Focus\ALM\log** directory.

To troubleshoot problems you may encounter while running the installation, see "Troubleshooting the installation" on page 222.

If you want to reconfigure OpenText Application Quality Management after the installation and configuration is complete, you must run the installation procedure again.

If an error occurs during the installation procedure, you must uninstall and restart the installation procedure.

If an error occurs during the installation procedure and the installation log file is not found, ensure that enough disk space is available for installation and deployment to the selected locations, and that system settings such as the open file resources limit are set to the maximum allowable value.

To install in Silent Mode:

> **Note:** To run silent installations for different configurations, you can create multiple configuration files.

1. Uninstall the existing version from the machine.
2. Create the **qcConfigFile.properties** file.

The file defines the configuration values that are used during the installation.

We recommend that you use an existing file from a prior installation.

If there is no existing file, you can create one manually. However, this can be a complicated process that is open to errors. We suggest that you create one by running a normal installation. During the installation process, the file is automatically created. The configuration values you define during the installation process are recorded in the file. Even if you subsequently uninstall, you can keep and edit the file as needed for future installations.

The file is automatically saved in the following path **C:\ProgramData\Micro Focus\ALM\conf** directory.

3. Update the **installer.properties** file with the installation path and the path of the configuration file, if they are not in their default locations.

> **Note:**
> - Neither the length of the file repository path nor the length of the deployment path can exceed 200 characters.
> - Due to a Windows limitation, the deployment directory and the repository path cannot be on a mapped drive.

4. If you want to use the Microsoft SQL Server (Windows Auth.) authentication type, do the following:
   a. In your JRE/JDK's bin folder, back up and remove the old mssql-jdbc_auth*.dll file if any.
   b. Copy the **mssql-jdbc_auth-8.2.2.x64.dll** file from the installer folder to your JRE/JDK's bin folder. If there is a jre folder under the JDK folder, copy the file to both the JDK/bin and JDK/jre/bin folders.
5. From the command line, run the **run_silent.bat** file.

If the installation process fails, check the installation logs for details. For details see "Checking the installation and configuration log files" on page 227.

If the installation process ends with warnings, the ALM server does not automatically start. Check the installation logs for details, and start the server manually. For details see "Checking the installation and configuration log files" on page 227.

Configure the IIS Mail Service

If you select **Microsoft IIS SMTP Service** as your mail server, you must configure the Microsoft IIS SMTP service as follows:

1. Open the Internet Information Services (IIS) Manager window.
2. In the Tree pane, right-click **Default SMTP Virtual Server** and select **Properties**. The Default SMTP Virtual Server Properties dialog box opens.
3. In the Access tab, click the **Connection** button. The Connection dialog box opens. Select **All except the list below** and click **OK**.
4. Click the **Relay** button. The Relay Restrictions dialog box opens. Select **All except the list below** and click **OK**.
5. Click **OK** to close the Default SMTP Virtual Server Properties dialog box.

Install on Linux systems

This section describes how to install OpenText Application Quality Management on Linux operating systems. It also describes how to install OpenText Application Quality Management silently.

> **Note:** For installation troubleshooting details, see "Troubleshooting the installation" on page 222.

This section includes:

Installation considerations: Linux

Before installing, consider the following:

Default paths	• **Installation path:** `/root/ALM` • **Server deployment path:** `/var/opt/ALM` • **Repository path:** `/var/opt/ALM/repository`
Paths and files created automatically by the ALM	• `/var/opt/Micro Focus/ALM/conf` • `/var/opt/Micro Focus/ALM/log` • `/var/opt/Micro Focus/ALM/runtime`
Logs	The locations of the **Site Administration** and **client** log files are subject to your settings. You can verify the locations from Site Administration. The **installation** log file is located in the server installation folder. The **deployment** log file is located in `/var/opt/Micro Focus/ALM/log`.

Installation scenarios	• **Upgrading from 15.x.x or earlier to 25.1.** When upgrading a copy of an existing Site Administration database schema, consider the following:
	  • If you are **using the existing settings as default**, the default deployment path will be the same as the path used in the previous installation. This path can be changed.
	  • If you are **not using the existing settings as default**, the default deployment path will be `/var/opt/Micro Focus/ALM`. This path can be changed.
	
	Note: The repository path of the upgraded projects will be the same as the path used in the previous installation.
	
	After upgrading, the newly created projects will use the repository path that was defined during the current installation.

Java path used	The variable `MICRO_FOCUS_JAVA_PATH` indicates the Java path used by OpenText Application Quality Management. The variable is added to `/etc/profile` (for 17.0) or `/etc/profile.d/MF_JAVA_PATH.sh` (for ALM 17.0.1 and later) during the ALM installation. If the **MF_JAVA_PATH.sh** file is not created during installation, manually create the file as the root user, add `export MICRO_FOCUS_JAVA_PATH=<JAVA_PATH>` in the file, and make it take effect by running `# source /etc/profile.d/MF_JAVA_PATH.sh`. If you need to start or stop the service manually, or if you need to install or uninstall a patch, verify that the `MICRO_FOCUS_JAVA_PATH` value and that the current session are both pointing to the path used by ALM. • To verify the path, run: `# cat /etc/profile` (for 17.0) or `# cat /etc/profile.d/MF_JAVA_PATH.sh` (for 17.0.1 and later). • To check it in your current session, run: `# echo $MICRO_FOCUS_JAVA_PATH`. If the output is empty, run: `# source /etc/profile` (for 17.0) or `# source /etc/profile.d/MF_JAVA_PATH.sh` (for 17.0.1 and later), or login with a new session, and try again.

Install on Linux

Before installing, consider the following:

- Verify that you meet the various installation prerequisites. For prerequisite information, see the relevant chapters in "Installation prerequisites" on page 33.
- If you are working in a clustered environment, you must mount the file system repository before you start the installation process. The mount should not use any cache mechanisms. For details, contact your network administrator.

- By default, the installation processes run in console mode. Navigating from one wizard step to the next requires familiarity with the various console mode command types. For explanations of the various command types and the methods for entering configuration settings, see "Work in Console Mode" on page 120.
- If you are planning to upgrade a copy of the existing Site Administration schema, the database server of the existing Site Administration schema and the database server of the existing Lab_Project must be supported. If these database servers are not supported, you can disable the validation check. For details, refer to "Disabling validation checks for the installation wizard" on page 222.

  > **Note:** For the most up-to-date supported environments, see the Support Matrix.

- If you encounter problems during the installation process, see "Troubleshooting the installation" on page 222 for troubleshooting suggestions.
- If you want to reconfigure after the installation and configuration is complete, you must run the installation procedure again.
- If an error occurs during the installation procedure, you must uninstall and restart the installation procedure.
- If an error occurs during the installation procedure and the installation log file is not found, ensure that enough disk space is available for installation and deployment to the selected locations, and that system settings such as the open file resources limit are set to the maximum allowable value.
- **$** is a reserved character in the installation procedure. For non-password fields use **$DOLLAR$**. For example, **$admin$** should be entered as **$DOLLAR$admin$DOLLAR$**. Password fields can continue to use **$**.

To install:

1. Log in to the host machine with the appropriate permissions. For a list of required permissions, see "Required Permissions: Linux" on page 41.
2. If OpenText Application Quality Management is installed on the machine, uninstall it. For information on uninstalling, see "Uninstall" on page 173.

   > **Cluster environment:** Uninstall ALM from all nodes.

3. The installation process can be run in console mode only.
4. Create an installation directory on the server. For example: **/usr/Install/ALM**.

   > **Note:** The installation cannot be executed using a path that contains "..", such as ./../../ALM/ALM_installer.bin

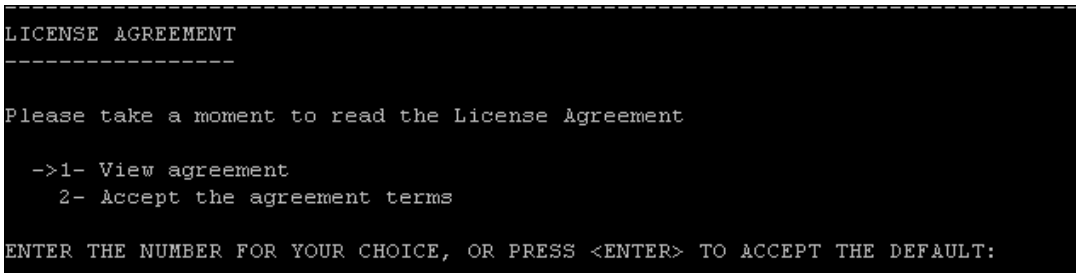
5. Navigate to the **/mnt/dvd/ALM-Linux** installation subfolder.
6. Copy the entire contents of the subfolder to the installation directory you created on the server.
7. Run the following **chmod** command to allow permissions for the installation files: **chmod -R 777 <installation directory>**.
8. From the installation directory on the server, navigate to the folder with the **ALM_installer.bin** file and run **ALM_installer.bin**.

   > **Note:**
   >
   > - The configuration settings are saved in the **qcConfigFile.properties** file.The file is created in the **/var/opt/ALM/conf** directory. The file should not be moved from this location.
   > - Also, the **repid.txt** file is created in the **<ALM Repository path>/qc** folder. The file should not be moved from this location.
   > - If you are installing on a secondary node of a cluster, some of the configuration dialog boxes that are needed only for the primary node are not displayed.

9. The Setup Wizard page opens, displaying the Welcome page.

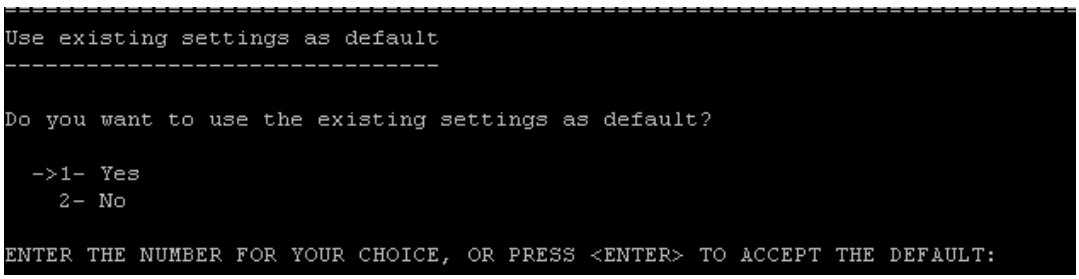
   Click **Enter** to continue.

10. The License Agreement page is displayed.



   Read the agreement. To accept the terms of the agreement, select **2**.

11. If the wizard detects settings from a previous installation, the Existing Settings page is displayed.



   By default, existing settings are used. The existing settings appear as defaults in subsequent wizard screens. You can then make changes to any of the settings.

   Choose to keep or clear the existing settings, then proceed to the next page.

12. The JDK/JRE Path page is displayed.

    Enter the JDK or JRE folder path.

> **Note:** ALM requires Java JDK or JRE to be installed prior to installing ALM. For details, see "Prerequisites: General" on page 58.

13. The Choose Install Folder page is displayed, displaying the default location for the installation files.

```
===============================================================================
Choose Install Folder
---------------------

Please choose a destination folder for this installation.

Where would you like to install?

  Default Install Folder: /root

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
      :
```

To keep the default installation folder, click **Enter**, or enter an absolute path to define another destination folder.

> **Note:** If you change the default, a soft link (symbolic link) with the default directory path is created that points to the directory you define.

14. The Database Server page is displayed.
    a. Select the database type.

```
-------------------------------------------------------------------------------
Database Server
---------------

Enter the database type

  ->1- MS-SQL (SQL Auth.)
    2- Oracle

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
```

    For details on database requirements, see "Prerequisites: Oracle Database Servers" on page 44 or "Prerequisites: Microsoft SQL Database Servers" on page 54.

    b. Select a database connection method.

```
-------------------------------------------------------------------------------
Database Connection
-------------------

Enter the database connection using database parameters or a connection string

  ->1- Database Parameters
    2- Connection String

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
```

    Select one of the following:

- **Database Parameters.** Enables you to enter database server information.
- **Connection String.** Enables you to type a formulated database server connection string.

Oracle RAC database	Select **Connection String**, and enter a connection string, specifying the folder that contains the **tnsnames.ora** file, and the TNS server to which ALM should refer. Use the following example: `jdbc:oracle:thin:@OrgRAC;oracle.net.tns_admin=/opt/oracle/tnsnameFolder` For details on prerequisites for Oracle RAC support, see"Oracle RAC Support" on page 52
Microsoft SQL Server database	If your database requires SSL/TLS access, see "Configure a secure database connection for a new installation" on page 165.

c. Enter Database Parameters.

If you selected the **Database Parameters** connection method above, enter the following information:

- **DB host name.** Type the database server name.

```
================================================================================
Database Parameters - DB Host Name
----------------------------------

Enter DB Host Name

DB host name :
```

- **DB port number.** Type the database server port number, or accept the default port number. To accept the default click **Enter**.

```
================================================================================
Database Parameters - DB Port
-----------------------------

Enter DB Port

DB port number (DEFAULT: 1433):
```

- **Oracle service name.** Type the Oracle service name.

```
--------------------------------------------------------------------------------
Database Parameters  - Oracle Service Name
----------------------------------------

Enter Database Service Name

Oracle service name (DEFAULT: ):
```

d. Enter Database Administrator Login information.

Specify the following:

- **DB admin user name.** The name of the user with the administrative permissions required to connect to the database server.

```
--------------------------------------------------------------------------------
DB Administrator Login
----------------------

Enter the database administrator username

DB admin user name (DEFAULT: sa):
```

- **DB admin password.** The database administrator password.

```
--------------------------------------------------------------------------------
DB Administrator Login
----------------------

Password to connect to the database

Enter database administrator password:
```

15. The Site Administration Database Schema page is displayed.

a. Select a Site Administration database schema option.

```
--------------------------------------------------------------------------------
Site Administrator Database Schema
----------------------------------

Select action

  ->1- Create a new schema
    2- Upgrade a copy of the existing schema
    3- Connect to the existing schema / second node

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:
```

Select one of the following:

Create a New Schema	Creates a new Site Administration database schema and a new Lab_Project. This is the default option. **Note:** The installation log and the enable_extensions.txt file contain error messages stating "Schema differences were found". These errors can be ignored, they are generated as part of the schema enable extension mechanism and the upgrade mechanism.
Upgrade a copy of the existing schema	Creates a copy of the existing Site Administration database schema, and upgrades the copy. For details, "Upgrade the Site Administration database schema" on page 69. If you select this option, you are prompted to add an exception file to the upgrade process. If you have defined an exception file, enter the location of where it was saved prior to the installation process. For details about exception files, see "Manage schema changes" on page 72. When working in a cluster environment, select this option if you have an existing primary node and you want to install OpenText Application Quality Management. **Note:** When you upgrade a copy of the existing Site Administration schema, OpenText Application Quality Management tries to copy LAB_PROJECT to the database server where the original LAB_PROJECT exists. If LAB_PROJECT is successfully copied, the new upgraded Site Administration schema points to the new copy of LAB_PROJECT. If LAB_PROJECT is not copied, a new empty LAB_PROJECT is created in the database server where the new Site Administration database schema is created. For details, see "LAB_PROJECT installation considerations" on page 121"LAB_PROJECT installation considerations" on page 121

Connect to existing schema / second node	This option can be used in two scenarios: ◦ If you are reinstalling and would like to reconnect to the same Site Administration database schema. ◦ If you have an existing node and you want to install on another node to create a cluster. For details on cluster configuration, see "Clustering: Linux" on page 43. **Note:** This option enables you to connect to a 25.1 Site Administration database schema only. To connect to an earlier version of Site Administration, you must first upgrade the schema. For details, see "Upgrade the Site Administration database schema" on page 69.

b. When creating a new schema, in **Database Name**, enter the name of the database.

c. Enter Oracle Tablespace information.

If you are using an Oracle database, enter the following information. If you are using a Microsoft SQL database, skip this step.

Note: If you are installing on a secondary node or if the Site Administration database already exists, the new Site Administration database schema is created in the same tablespace as the existing schema. Continue with the Security step below.

◦ **Default Tablespace.** The Default Tablespace is the location on the database where database objects will be created.

- **Temporary Tablespace.** The Temporary Tablespace is the location on the database where temporary tables are created to facilitate internal database functionality, such as large sorting tasks. We recommend that you accept the default location.

```
-------------------------------------------------------------------------------
Oracle Temporary Tablespace Selection
-------------------------------------

  ->1- TEMP

Choose Oracle temporary tablespace:
```

d. Enter Site Administration database schema details.

   Enter the following information:

   - **Schema name.** Enter a name for the Site Administration database schema, or accept the default. The Site Administration database schema name can only contain English characters or numbers.

```
-------------------------------------------------------------------------------
SA Schema Name
--------------

Enter Site Admin schema name

SA schema name (DEFAULT: sa_12_172):
```

     If you selected **Upgrade a copy of the existing schema** above, the **New Schema Name** option appears. Type a name for the upgraded copy of the Site Administration database schema.

> **Note:** When upgrading an existing Site Administration database schema to work in 25.1, you must use the same name that you used before the upgrade.

   - **Schema password.** Enter the following information, depending on your database type:

```
-------------------------------------------------------------------------------
SA Schema Password
------------------

SA schema password

Enter Site Admin schema password:
```

- **Oracle.** The default **tdtdtd** password is created, which you can accept or change.
- **Microsoft SQL Server (SQL Auth.).**OpenText Application Quality Management uses the **td** user to create the Site Administration database schema. For more details on the **td** user, see"User Permissions for Connecting to a Microsoft SQL Database Server" on page 55.

  Type a password for the **td** user that complies with your organization's password policy, or keep the default **tdtdtd** password.

16. The License Key page is displayed.

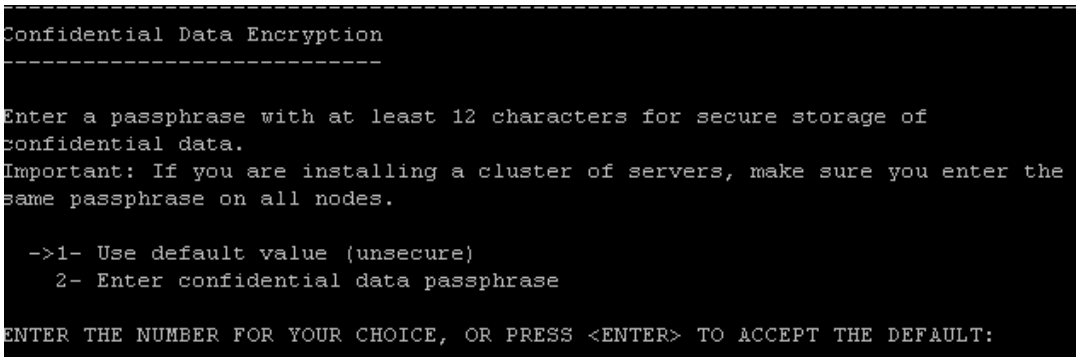
    Note: If you selected **Connect to existing schema / second node** in the previous step, the License Key step is skipped. Continue with the Security step below.

    Select one of the following options:

Insert License file	Select **1** to enter the License file path. Enter the ALM License file path.

Use Evaluation Key	Select **2** to use an Evaluation Key. If you do not have a License key, you can use an evaluation key for a 30-day trial version . A list of available editions is displayed. From the editions list, choose the edition you want to use. **Note:** If you install OpenText Quality Center Community Edition, you must assign named licenses to your users. Only then can the users successfully log in to ALM and see the appropriate modules. For details on assigning named licenses, see the ALM online help.
Use License Server (Technical Preview)	Select **3** to use the AutoPass License Server (APLS). a. Enter the license server address. b. Enter the license server port. c. Enter license server protocol. Alternatively, you can also configure APLS after the ALM installation. Perform the following steps: a. From the ALM server machine, navigate to `/var/opt/ALM/repository/sa/Admin/MaintenanceData/conf` b. Edit `clusterSettings.properties` c. Define values for the following fields: AUTOPASS_SERVER_PROTOCOL, AUTOPASS_SERVER_PORT, AUTOPASS_SERVER_NAME. d. Save and restart the ALM server.

17. The Security page is displayed.



Passwords for accessing external systems (databases and LDAP) are stored after encryption. Enter a Confidential Data Passphrase that OpenText Application Quality Management uses to encrypt the information or choose to use the default value. If you use the default value however, the encrypted information is more vulnerable to unauthorized access.

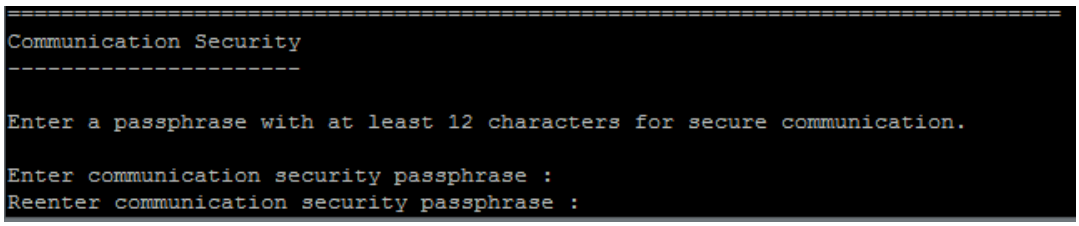
Make a note of the passphrase for future support calls. You will also need the passphrase if you choose to redeploy or choose to upgrade a copy of the existing Site Administration Database Schema, or whenever you upgrade the version.

Confidential Data Passphrase Considerations

- You must enter the same passphrase that was used for the previous installation. If you do not know the passphrase, there is a workaround to recover it. However, you have to abort the configuration process and then begin again once the workaround is complete. For details, see "Recover a lost confidential data passphrase" on page 71.
- If you are planning to migrate, restore, or import extension-enabled projects (such as LoadRunner Enterprise and/or Lab Management enabled projects)onto the server on which you are performing the installation, you must use the same Confidential Data Passphrase that was defined on the server on which the projects were created.
- If you are installing on a cluster, you must use the same passphrase for all nodes.
- After completing the server installation wizard, you cannot change the confidential data encryption passphrase.
- The passphrase is case-sensitive. Check that there are no empty spaces before or after the passphrase. The passphrase must contain only alphanumeric characters.

> **Caution:** If you use a different passphrase than that for the previous version, stored information such as API key secrets, SMTP passwords, and database server passwords become invalid and cannot be restored. This results in connection failures to all ALM projects and the corresponding systems.

18. Enter a Communication Security Passphrase.



Communication between OpenText Application Quality Management and other OpenText applications is enabled after authentication by a Single Sign-On (SSO) token. Enter a Communication security passphrase that is used to encrypt the SSO token.

> **Note:**
> - The communication security passphrase is stored as the value of the **COMMUNICATION_SECURITY_PASSPHRASE** site configuration parameter. For details, refer to the online help.
> - The passphrase must contain only alphanumeric characters, and must contain at least 12 characters.
> - **LoadRunner Enterprise:** You must use the same communication security passphrase for the LoadRunner Enterprise server configuration.

Communication Security Passphrase considerations

- You must enter the same passphrase that was used for the previous installation.
- If you are planning to migrate, restore, or import extension-enabled projects onto the server on which you are performing the installation, you must use the same passphrases that were defined on the server on

the original server.

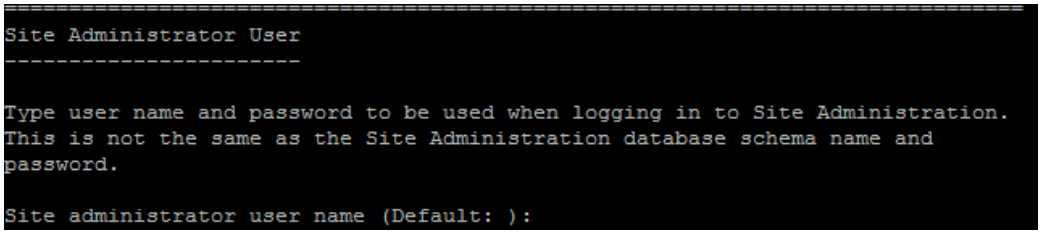
- If you are installing on a cluster, you must use the same passphrase for all nodes.

> **Caution:** If you use a different passphrase than that for the previous version, stored information such as API key secrets, SMTP passwords, and database server passwords become invalid and cannot be restored. This results in connection failures to all projects and the corresponding systems.

19. Enter Site Administrator Login information.

    Specify the following:

    - **Site Administrator user name.** The Site Administrator user name.



    - **Site Administrator password.** The Site Administrator password.

      After entering the Site Administrator password, you are prompted to re-enter the password.

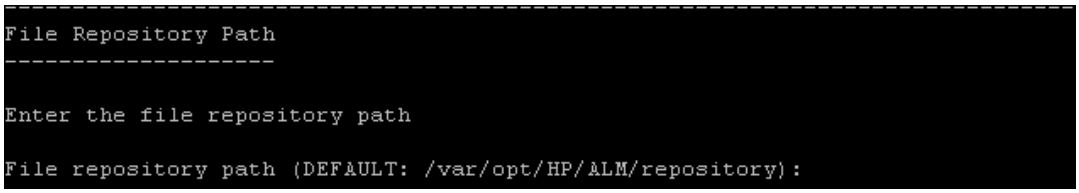
    You use the site administrator name and password that you define here to log in to Site Administration. After installation, you can change the site administrator or add other site administrators. Enter a site administrator

user name (maximum length 60 characters) and password, and retype the password to confirm.

If you are upgrading a copy of the existing Site Administration database schema, by default the same user and credentials are applied to the upgraded Site Administration database schema. The **Create additional Site Administrator user** option is displayed, enabling you to ignore this default and create an additional user.

> **Note:**
> - The user name cannot include the following characters: **\ / : * ? " < > |**
> - The password cannot be longer than 20 characters.
> - It is important that you remember the site administrator user name and password as otherwise you cannot log in to Site Administration.

20. The File Repository Path page is displayed.



Accept the default path or enter a new path. If you choose to ignore the default, make sure to enter a unique case-sensitive path.

> **Note:**
> - Make sure you select a path where you have full read and write permissions.
> - To work with cluster nodes, make sure that all nodes have access to the file repository path and that the path is UNC. All nodes in the cluster must have the same repository path.
> - The length of the file repository path cannot exceed 200

characters.

- The file repository path cannot reside on the root folder.

Using the **BASE_REPOSITORY_PATH** site configuration parameter, you can create a location for a repository path where new projects will be located. Performing this action, results in the creation of two repository paths - the previous path containing older projects, and a second path containing projects created subsequently. For details, refer to the online help.

21. The Application Server page opens.
    a. Enter Deployment Path information.

    Enter a **Deployment Path**, where you specify the location in which you want to deploy application files. We recommend that you keep the default.

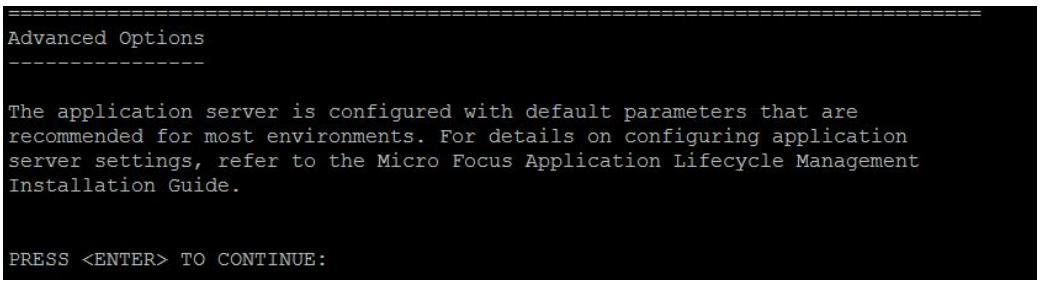
> **Note:** The length of the deployment path cannot exceed 200 characters.

    b. Enter Web server information.

    Change or keep the default HTTP port number. The default port is 8080.

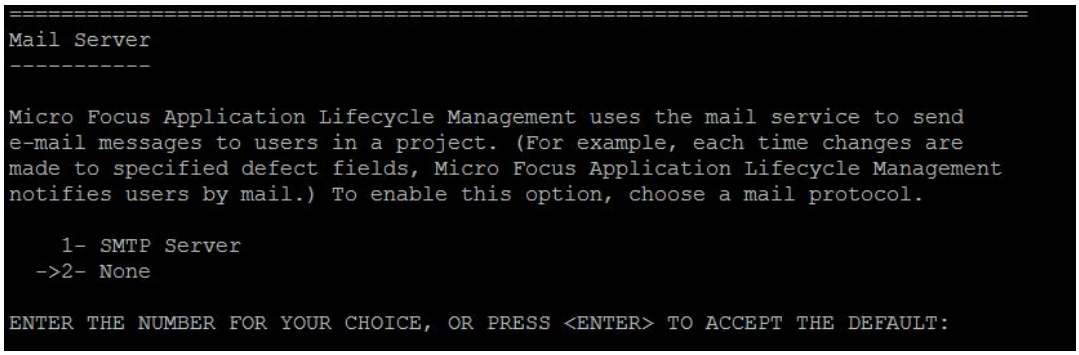
> **Note:** If an error message is displayed that the default port is unavailable, it may be the port is in use by another application running on the server machine. Either locate the application and stop it, or enter a different port number. To enter a different port number, you must first change the port number on the application server. For details, see . Then proceed with the configuration as normal.

c. The Advanced Options page opens.



Click **Enter** to continue.

22. The Mail Server page is displayed.

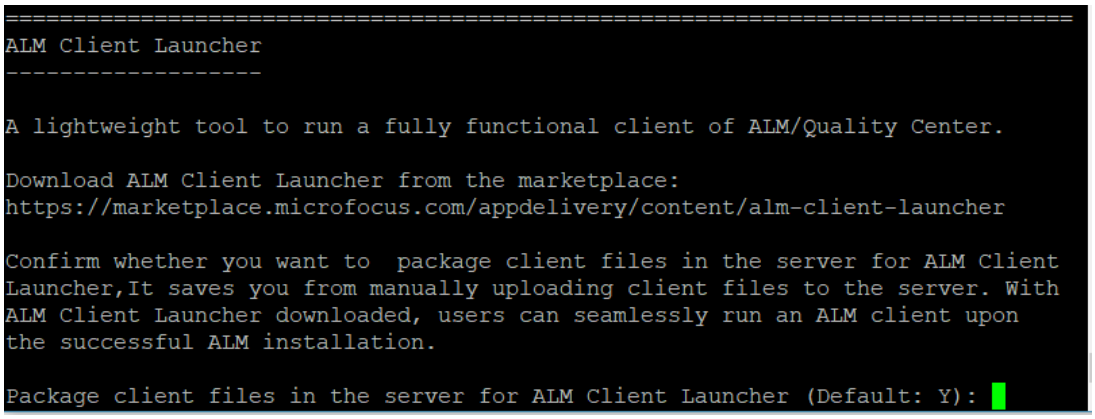


To enable OpenText Application Quality Management to send emails to users in a project, choose **SMTP Server**. Then when prompted, enter the server name.

> **Note:** The Mail Server can be configured after installation in Site Administration. For details, refer to the ALM online help..

23. The Start ALM Server page is displayed. To keep the default option, click **Enter**.

24. The ALM Client Launcher page is displayed.



From this page, you can:

- Use the marketplace link to download ALM Client Launcher and learn more about the tool.

  You can also download ALM Client Launcher after the ALM installation.

- Enter Y in the **Package client files in the server for ALM Client Launcher** option to have client files automatically packaged in the server.

  We recommend that you package client files if you want to use ALM Client Launcher. It saves you from manually uploading client files to the server. Users that have downloaded ALM Client Launcher can seamlessly run an ALM client upon the successful ALM installation.

25. The Installation Summary page is displayed. To change any settings, enter **Back**.

    Understand the breaking changes in this version and acknowledge all the breaking changes to continue.

    To apply the settings and start the configuration process, click **Enter**.

26. The Finish page is displayed.

If the installation process fails, check the installation logs for details. For details, see "Checking the installation and configuration log files" on page 227.

If you selected to upgrade a copy of the existing Site Administration database schema, it is possible that an upgrade related issue caused the configuration to fail. Check the following files located in the **<file repository path>/sa/Admin/maintenancedata/out** directory for more information:

- **upgrade.txt**
- **verifyreport.html**

If the failure was due to changes made to the existing Site Administration database schema and the upgraded server will work properly with these Site Administration database schema changes, you need to create an exception file that excludes these changes from the upgrade process. Then run the installation again, using the current settings. For details, see "Manage schema changes" on page 72.

27. If you are prompted to restart your machine you can choose to restart at a later time but you must restart before you use OpenText Application Quality Management. You must also restart before you install any related files, such as integration add-ins.

    If choose not to restart the ALM server during installation, make sure to run `source /etc/profile` to prevent the ALM service from failing to start. Alternatively, re-login with a new session.

28. If you are using an Oracle RAC database, verify that the **ORACLE_RAC_SUPPORT** site configuration parameter is set to **Y**. For details, refer to the

online help.

29. The installation is now complete. Proceed to "Starting the system" on page 123

Install in silent mode on Linux

A silent installation runs the entire setup process in the background without requiring you to navigate through setup screens and input selections. Instead, all configuration parameters are assigned values that you define in a configuration file (**qcConfigFile.properties**). When running an installation in silent mode, no messages are displayed. Instead, you can view installation information in the log file, including information on whether the installation was successful. The installation log file can be found under the **<installation folder>/log** directory. The deployment and configuration log file can be found under the **/var/opt/ALM/log** directory.

To troubleshoot problems you may encounter while running the installation, see "Troubleshooting the installation" on page 222.

If you want to reconfigure OpenText Application Quality Management after the installation and configuration is complete, you must run the installation procedure again.

If an error occurs during the installation procedure, you must uninstall and restart the installation procedure.

If an error occurs during the installation procedure and the installation log file is not found, ensure that enough disk space is available for installation and deployment to the selected locations, and that system settings such as the open file resources limit are set to the maximum allowable value.

$** is a reserved character in the installation procedure. For non-password fields use **$DOLLAR$**. For example, **$admin$** should be entered as **$DOLLAR$admin$DOLLAR$**. Password fields can continue to use **$.

To install in Silent Mode:

> **Note:** To run silent installations for different configurations, you can create multiple configuration files.

1. Uninstall any previous installations of Quality Center or ALM from the server machine.
2. Create the **qcConfigFile.properties** file.

   The file defines the configuration values that are used during the installation.

   We recommend using an existing file from a prior installation.

   If there is no existing file, you can create one manually. However, this can be a complicated process that is error-prone. We suggest that you create one by running a normal installation. During the installation process, the file is automatically created. The configuration values you define during the installation process are recorded in the file. Even if you subsequently uninstall OpenText Application Quality Management, you can keep and edit the file as needed for future installations.

   The file is automatically saved in the following path **/var/opt/ALM/conf**.
3. Create an installation directory with read and write permissions on the server, for example: **/usr/Install/ALM**

   > **Note:** The installation cannot be executed using a path that contains "..", such as ./../../ALM/ALM_installer.bin
4. Under the mount folder, navigate to the **/mnt/dvd/ALM-Linux** installation subfolder.
5. Copy the entire contents of the subfolder to the installation directory you created on the server.
6. Run the following chmod command to allow permissions for the installation files: **chmod -R 777 <installation directory>**

7. Update the **installer.properties** file with the installation directory and the path of the configuration file, if the configuration file is not in the default path.

   > **Note:** Neither the length of the file repository path nor the length of the deployment path can exceed 200 characters.

8. From the installation directory on the server, navigate to, and run the **run_silent.sh** file.

Work in Console Mode

By default, the Server Installation Wizard runs in console mode. Navigating from one wizard step to the next requires familiarity with the various console mode command types. This section explains the various command types and the methods for entering configuration settings.

List Options

Some wizard screens present a set of options in the form of a list, where you can select only one option. For example:

```
-------------------------------------------------------------------------------
Database Server

Database Type

[X] 1 - MS-SQL (SQL Auth.)
[ ] 2 - Oracle

To select an item enter its number, or 0 when you are finished: [0]
```

To make your selection, type the numeric value of the option you want to select, then press **Enter**.

The page appears again, this time with the checkmark placed by the option you selected. In this example, if you enter **2**, then press **Enter**, the following appears:

```
--------------------------------------------------------------------------------
Database Server

Database Type

[ ] 1 - MS-SQL (SQL Auth.)
[X] 2 - Oracle

To select an item enter its number, or 0 when you are finished: [0]
```

To confirm your selection, type **0** then press **Enter**.

Text Options

Some wizard screens require you to enter text. For example:

```
DB port number:
```

If the wizard detects a pre-existing value for the required field, or if there is a default value, that value appears in brackets. For example:

```
DB port number: [1521]
```

To ignore the existing value, type a new value then press **Enter**. The new value overrides the existing value.

To keep the current value, or leave the field empty, press **Enter**. The following option appears:

```
Press 1 for default value, or 2 for no value: [1]
```

To proceed to the next step with the existing value, type 1 then press **Enter**.

To proceed to the next step and leave the field empty, type 2 then press **Enter**.

LAB_PROJECT installation considerations

When you select **Upgrade a copy of the existing schema** in the Installation wizard, OpenText Application Quality Management tries to copy LAB_

PROJECT as well. Below is a more detailed explanation of the actions performed on LAB_PROJECT when upgrading a copy of the existing Site Administration schema:

1. OpenText Application Quality Management tries to copy LAB_PROJECT to the database server where the original LAB_PROJECT exists.

   If LAB_PROJECT is successfully copied:

   - The new Site Administration schema points to the new LAB_PROJECT.
   - The copied LAB_PROJECT has an empty repository. You need to copy the repository from the source LAB_PROJECT.
   - The copied LAB_PROJECT must be upgraded.

2. If OpenText Application Quality Management fails to copy LAB_PROJECT to the database server where the original LAB_PROJECT exists, a new empty LAB_PROJECT is created in the database server where the new Site Administration database schema is created.

   To copy the original LAB_PROJECT data to make it usable for the installation:

   - Remove the new LAB_PROJECT.
   - Create a copy of the original LAB_PROJECT database schema and repository:
     - Backup the original LAB_PROJECT database schema.
     - Restore a backup of the original LAB_PROJECT into the new installation database server.
     - Copy the source repository from the original LAB_PROJECT into the new installation repository.
   - Update the **dbid.xml** file of the new LAB_PROJECT with the new:
     - Installation database server name
     - Connection string
     - Password
     - Repository location

- Restore the new LAB_PROJECT.
- Upgrade the new LAB_PROJECT.

Starting the system

This section introduces OpenText Application Quality Management options and resources. It also explains how to start OpenText Application Quality Management.

Windows - browsing the program folder

In Windows, after the setup process is complete, the following items are added to your program folder (**Start > Programs > ALM Server**):

Option (A-Z)	Description
OpenText Application Quality Management Tray Icon	Places the system tray icon in the system tray if it does not appear there.
OpenText Application Quality Management	Opens OpenText Application Quality Management. For details, see Use
Site Administration	Opens the Site Administration application. For details, see Admin.
Uninstall OpenText Application Quality Management	Uninstalls OpenText Application Quality Management. For details, refer to "Uninstall" on page 173.

Windows - starting and stopping services

In the system tray, right-click the OpenText Application Quality Management icon and select **Start OpenText Application Quality Management**, or **Stop OpenText Application Quality Management**

Starting on a Client Machine

You launch OpenText Application Quality Management on your client machine using either ALM Client Launcher or Microsoft Edge with IE mode enabled.

Before logging in, you must first create a project in Site Administration. For details, refer to the *the help*.

> **Note:**
>
> - To enable OpenText Application Quality Management to work with OpenText testing tools as well as third-party and custom tools, you must run the ALM Client Registration add-in, which registers client components on the client machine. For details, see "Registering on a Client Machine" on page 127.
> - If your users connect to OpenText Application Quality Management over a virtual environment, such as Citrix or VMware, you can deploy client components on a shared location that all users can access. To enable a shared deployment, run the **Shared Deployment for Virtual Environments** add-in. For details on installing add-ins, refer to the *the help*.

To start using ALM Client Launcher:

1. Enter your OpenText Application Quality Management URL in your browser.
   `http://<OpenText Application Quality Management server name/IP address>[<:port number>]/qcbin`. Contact your system administrator if you do not have the correct URL.
2. For Single-Sign-On users:
   a. If the user discovery page is displayed, add your user name or email address as specified in ALM. Click **Submit**.
   b. In the IDP page, add your IDP credentials. Click the log in button.

3. In the OpenText Application Quality Management Options window, click **OpenText Application Quality Management Desktop Client** link.
4. If you already have ALM Client Launcher installed, click **Open ALM Client Launcher** in the confirmation dialog box.
5. If you did not install ALM Client Launcher, from the Download ALM Client Launcher page, select where to download ALM Client Launcher, from Marketplace or ALM Server, and click **Download**. Save the download file and run it.

   For details about how to use ALM Client Launcher, see the online help.
6. In the login page, provide the following information:

User name	Enter your username. Not available for Single-Sign-On users.
Password	Enter the password assigned to you by your site administrator. **Available in 16.0.1 and later:** You can click and hold the eye icon (👁) next to your password to show it in plain text. Not available for Single-Sign-On users.
Forgot Password	If you cannot remember your password, click link to reset your password. Not available for Single-Sign-On users.
Automatically log in to my last domain and project on this machine	Select check box if you want OpenText Application Quality Management to automatically log in to the last project in which you were working. Not available for Single-Sign-On users.

Authenticate	Click to verify your user name and password. OpenText Application Quality Management determines which domains and projects you can access. If you specified automatic login, OpenText Application Quality Management opens. If authentication fails, check that your user name and password are correct and try again. **Note:** • If authentication fails multiple times, you can be locked out of ALM. The number of authentication attempts you are allowed is determined by your site administrator. • Not available for Single-Sign-On users.
Domain	Select a domain. By default, the last domain in which you were working is displayed.
Project	Select a project. By default, the last project in which you were working is displayed.
Login	OpenText Application Quality Management opens and displays the module in which you last worked during your previous session. The first time you run OpenText Application Quality Management, the Welcome page opens. When a user session is inactive for a period of time, the session expires. This releases the license in use, making it available for other users. When a session expires, you are prompted to reconnect. You can edit reconnect options by modifying the **FAST_RECONNECT_MODE** parameter in the Site Configuration tab. This parameter is not valid for external authentication, since the user must always be certified when reconnecting.

For details about accessing using Microsoft Edge IE mode, see the online help.

Registering on a Client Machine

To enable you to work with other OpenText testing tools as well as third-party and custom tools, OpenText Application Quality Management must be registered on the client machine. To register it, run **ALM Client Registration** from the Tools page.

> **Note:** If you are running previous versions on your machine, before registering 25.1, make sure that all instances and any integration tools are closed.

Tools that Require Registering ALM Client Components

The following tools require that client components be registered on the client machine:

Add-ins	• OpenText Functional Testing Add-in
	OpenText OpenText Functional Testing (OpenText Functional Testing) comprises the product formerly known as QuickTest Professional and the product known as Service Test.
	  • Functionality provided by QuickTest is now known as GUI testing in OpenText Functional Testing.
	  • Functionality provided by Service Test is also known as API testing in OpenText Functional Testing.
	
	Note: Windows 7: Requires that Data Execution Prevention (DEP) be disabled.
	
	• OpenText Screen Recorder Add-in
	• Service Test Add-in
	• ALM Synchronizer

Other	OpenText Functional Testing tests OpenText OpenText Functional Testing (OpenText Functional Testing) comprises the product formerly known as QuickTest Professional and the product known as Service Test. • Functionality provided by QuickTest is now known as GUI testing in OpenText Functional Testing. • Functionality provided by Service Test is also known as API testing in OpenText Functional Testing. **Note:** • Required to run tests. • Windows 7: Requires that Data Execution Prevention (DEP) be disabled.

Integrating with a web server

To enhance the security of your OpenText Application Quality Management deployment, we recommend placing the server behind a secure reverse proxy, either an Apache or IIS web server. Such configuration is also required to support external authentication. If you are not using a secure reverse proxy, we recommend configuring SSL on the server itself. For details on configuring SSL, see "Manage the application server" on page 137.

Configuring IIS as a reverse proxy

To integrate OpenText Application Quality Management with a web server, you configure the web server to redirect requests to the OpenText Application Quality Management Application Server. You configure the web server to work in proxy HTTP mode.

To configure IIS to work as a reverse proxy:

> **Note:** The following instructions apply to IIS 7.0 and later.

1. Using Server Manager, install the IIS server using default settings. You do not need to enable any other extensions.
2. Install the URL rewrite package.
3. Install Application Request Routing (ARR) for IIS.

   > **Note:** If you have no direct access to the internet from your server, you can obtain the ARR 3.0 standalone version that contains everything you need, including the URL rewrite package. Download ARR 3.0 to your client, copy it to the server, and install it on the server.

4. Make sure the IIS Web server is stopped.
5. Open IIS Manager and ensure you have an element named **Server Farms** under the relevant IIS server node.

   > **Note:**
   > - If there is no **Server Farms** element and you are using a Windows 2012 server, uninstall Microsoft Web Farm Framework and download the latest version.
   > - If you fail to install a Web Farm for IIS 10, see this KB article.

6. Right click **Server Farms** and click **Create Server Farm**.
7. Enter a name for the farm and click **Next**.
8. Click **Advanced settings** and change the ports to match your OpenText Application Quality Management Jetty ports. The default ALM Jetty ports are 8080 for http and 8443 for https.
9. Under **Server address**, type the name or IP address of the OpenText Application Quality Management server you want to add to the farm.
10. Click **Add** to add the server.

> **Note:** Repeat steps 9 - 10 to add more ALM servers to use IIS as a load balancer in an ALM cluster.

11. Click **Finish**.
12. Click **Yes** in the **Rewrite Rules** dialog box that opens. This adds a URL rewrite rule that causes IIS to forward all incoming requests to the ALM Server.
13. Select the new Server farm element created.
14. Double-click **Proxy**.
15. Set **Time-out (seconds)** to 35.
16. Set **Response buffer threshold** to 0.
17. Click **Apply**.

> **Note:** This change is applied only to the Application Request Routing proxy.

18. Enable the proxy.
    a. Select the main tree node (the server name), click **Application Request Routing Cache**, and then click **Server Proxy Settings** in the **Proxy** section.
    b. Enable **Enable proxy**.
    c. Verify that **HTTP version** is valued with **Pass Through**.
    d. Verify that **Reverse rewrite host in response headers** is enabled.
    e. Click **Apply**.
19. Restart the IIS Web server.

    You can now connect to your OpenText Application Quality Management site using the following URL: **http://<IIS server name>/qcbin**.
20. If you are using IIS with multiple servers farms:

a. Add another server farm for the other server group.
b. Modify the URL Rewrite rule for the ALM server farm:
    i. Select the main tree node (the server name) and click **URL Rewrite**.
    ii. Edit the **Inbound Rule**.
    iii. Change **Using** from **Wildcards** to **Regular Expressions**.
    iv. Change **Pattern** to **(^qcbin(.*))**.
    v. Click **Apply**.
c. Modify the URL Rewrite rule for the other server farm:
    i. Select the main tree node (the server name) and click **URL Rewrite**.
    ii. Edit the **Inbound Rule**.
    iii. Change **Using** from **Wildcards** to **Regular Expressions**.
    iv. Change **Pattern** to reflect the other server group.
    v. Click **Apply**.
d. Restart the IIS Web server.

Configuring IIS as a Secure Reverse Proxy

To configure IIS to work as a secure reverse proxy:

> **Note:** For detailed instructions, refer to the IIS documentation.

1. Ensure that you configured IIS to work as a reverse proxy.
2. Install the server certificate in IIS.

    > **Note:** The server certificate must have a password protected private key.

    In IIS Manager:

- Import your server certificate:

  Select **Server > Certificates > Import**.

- Add a listener on a secure port:

  Select **Default Website**.

  Edit **Bindings**.

  Click **Add**.

  Select **https** and select your certificate.

3. In **SSL Settings** for your website, configure IIS to require an SSL connection.
4. Verify that you can access the OpenText Application Quality Management server through the IIS virtual IP using the https protocol.

Configuring the IIS Web Server for SSL Offloading

SSL Offloading means that IIS is configured to connect to ALM over http and not https. In this case, perform the following configuration:

1. Edit the **qcbin** inbound rule and add the following server variable:

   Set **name="HTTP_X_FORWARDED_PROTO" value="https"**.

2. In **Action Properties**, change the protocol from https to http.
3. Restart IIS so it will read the configuration.

Configuring Apache as a reverse proxy

To configure Apache to work as a reverse proxy:

> **Note:**
> - Windows: It is recommended that you use Apache HTTP Server version 2.2.

- Linux: It is recommended that you use Apache HTTP Server version 2.4.

1. Make sure the Apache Web server is stopped.
2. Navigate to the **<Apache Home directory>\conf** directory.
3. Create a backup copy of the **httpd.conf** file.
4. Open the **httpd.conf** file.
5. Uncomment or add the following load module commands:

```
LoadModule proxy_module modules/mod_proxy.so

LoadModule proxy_http_module modules/mod_proxy_http.so

LoadModule rewrite_module modules/mod_rewrite.so

LoadModule headers_module modules/mod_headers.so
```

6. Add the following section to the end of the file:

```
# Turn off support for true Proxy behavior as we are acting
as
# a reverse proxy
ProxyRequests Off
# Turn off VIA header as we know where the requests are
proxied
ProxyVia Off
# Set the permissions for the proxy
<Proxy *>
AddDefaultCharset off
Order deny,allow
Allow from all
</Proxy>
# Turn on Proxy status reporting at /status
# This should be better protected than: Allow from all
ProxyStatus On
<Location /status>
SetHandler server-status
```

```
Order Deny,Allow
Allow from all
</Location>
# Configuring mod_proxy_http
# To connect to servlet container with HTTP protocol, the
ProxyPass
# directive can be
# used to send requests received on a particular URL to a
Jetty instance.
ProxyPreserveHost off
ProxyPass /qcbin http://<ALM server name>:8080/qcbin
ProxyPassReverse /qcbin http://<ALM server name>:8080/qcbin
# For OpenText Enterprise Performance Engineering
deployments, add the following:
ProxyPass /loadtest http://<LoadRunner Enterprise server
name>/loadtest
ProxyPass /LoadTest http://<LoadRunner Enterprise server
name>/LoadTest
ProxyPass /Loadtest http://<LoadRunner Enterprise server
name>/Loadtest
ProxyPassReverse /loadtest http://<LoadRunner Enterprise
server name>/loadtest
ProxyPassReverse /LoadTest http://<LoadRunner Enterprise
server name>/LoadTest
ProxyPassReverse /Loadtest http://<LoadRunner Enterprise
server name>/Loadtest
# Rewrite rule trailing slash must be used in the
VirtualHost section
RewriteEngine On
# Add trailing slash if was not present in the original
request
RewriteRule ^/qcbin$ /qcbin/ [R]
```

7. Save the changes to the file.
8. Run **httpd -t** from the Apache bin folder to check the syntax of the file.
9. Restart the Apache Web server.

You can now connect to your OpenText Application Quality Management site using the following URL: **http://<ALM virtual server name>[:<apache port number>]/qcbin**.

Configuring Apache as a Secure Reverse Proxy

To configure Apache to work as a secure reverse proxy:

1. Open the **httpd.conf** file.
2. Uncomment **ssl_module**:

```
LoadModule ssl_module modules/mod_ssl.so
```

3. Uncomment the **httpd-ssl.conf** file:

```
# Secure (SSL/TLS) connections
Include conf/extra/httpd-ssl.conf
```

4. Close the **httpd.conf** file and open the **httpd-ssl.conf** file. By default it is in **/<apache-directory>/conf/extra**.
5. In the httpd-ssl.conf file, activate the SSL port 443:

```
Listen 443
```

6. Add the **SSLProtocol** parameter:

```
SSLProtocol -SSLv2 -SSLv3 +TLSv1
```

7. Change the cache settings:

```
LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
SSLSessionCache "shmcb:<apacheAbsoluteFolder>/logs/ssl_
scache(512000)"
```

8. Modify the **VirtualHost** and **ServerName** parameters:

```
<VirtualHost <fully qualified server name>:443>
ServerName <fully qualified server name>:443
```

9. Add the SSL certificates to the **VirtualHost** section:

```
# Server Certificate
SSLCertificateFile " /<apache-
directory>/conf/WebServerPublicCert.pem"
# Server Private Key:
SSLCertificateKeyFile " /<apache-
directory>/conf/WebServerPrivateCert.pem"
```

10. Restart Apache so it will read the new configuration.

    Run **<apache-directory>/bin/apachectl -k restart**

11. Verify that Apache works as a secure proxy server.

    Go to **https://webserver/qcbin**. Make sure the OpenText Application Quality Management home page is displayed.

> **Note:** The web server name must be in FQDN (fully qualified domain name) format when using a secure connection.

12. After verifying that Apache works as a secure proxy server, close the non-secure port.

    a. Open the **httpd.conf** file.

    b. Comment out the **Listen** parameter:

```
#Listen 80
```

Configuring the Apache Web Server for SSL Offloading

SSL Offloading means that Apache is configured to connect to ALM over http and not https. In this case, perform the following configuration:

1. Navigate to the **<Apache Home directory>\conf** directory.
2. Create a backup copy of the **httpd.conf** file.
3. Open the **httpd.conf** file.
4. Add the following section if encrypted communication terminates on the Apache server:

```
#################################################################
###
# add the following line if SSL is terminated/offloaded on
Apache server

#################################################################
###
RequestHeader set X-Forwarded-Proto https
```

5. Save the **httpd.conf** file.
6. Restart Apache so it will read the configuration.

Manage the application server

This section contains information relating to managing the application Server, as well as information regarding general Java management tools.

Change the Heap Memory Size

After you install OpenText Application Quality Management, you may need to change the heap memory values. For example, you may want to increase the heap size if there is an increase in the number of active projects, or an increase in the number of concurrent user sessions.

> **Note:**
> - The maximum heap value cannot exceed your maximum memory (RAM) size.
> - On a machine running on a 32-bit operating system, the heap memory size should not exceed 1024 MB.

To change the heap memory size:

1. Verify that all users have logged out of projects and stop the service.

OS	Steps
Windows	In the system tray, right click the OpenText Application Quality Management icon and choose **Stop Application Lifecycle Management**.
Linux	Navigate to the **<ALM deployment path>/wrapper** directory, and run the following command: **HPALM stop**.

2. In the **deployment**path, open the **wrapper.conf** file.
3. Change the **wrapper.java.maxmemory** value as necessary.
4. Restart the service.

OS	Steps
Windows	In the system tray, right click the OpenText Application Quality Management icon and choose **Start Application Lifecycle Management**.
Linux	Navigate to the **<Deployment path>/wrapper** directory, and run the following command: **HPALM start**.

Change the Application Server Port Number

After you install, you may need to change the application server port number.

It is possible that the default application server port may be in use 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 application server port on the machine.

To change the application server port number:

1. Verify that all users have logged out of projects and stop the service.

OS	Steps
Windows	In the system tray, right click the OpenText Application Quality Management icon and choose **Stop Application Lifecycle Management**.
Linux	Navigate to **<Deployment path>/wrapper** directory, and run the following command: **HPALM stop**.

2. Navigate to the **<Deployment path>/server/conf/jetty.xml** file.
3. Change the **jetty.port** value.
4. Start the service.

OS	Steps
Windows	In the system tray, right click the OpenText Application Quality Management icon and choose **Start Application Lifecycle Management**.
Linux	Navigate to the **<Deployment path>/wrapper** directory, and run the following command: **HPALM start**.

Configure Secure Access

You can configure a secure connection to and from OpenText Application Quality Management. For more details, see "Configure secure access on Windows systems" on the next page or "Configure secure access on Linux systems" on page 149.

Configure Secure Database Access

This section describes how to configure a secure connection, such as Secure Socket Layer (SSL), from the OpenText Application Quality Management server to the database server. For more details, see"Configuring secure database access" on page 156.

Application Server Management Tools

The OpenText Application Quality Management Application Server is Java-based. Therefore, we recommend the following Java tools for effective application server management:

- JConsole
- JStack
- JMap
- JVisualVM

> **Note:** JVisualVM is an all-in-one tool that was added in Java 1.6. However JVisualVM is very memory and CPU intensive, so you may find that another tool is more useful.

Configure secure access on Windows systems

This topic describes how to configure a secure connection to and from OpenText Application Quality Management when it is installed on a Windows system. For the procedure, see "Configure a secure connection to the application server (Jetty)" on the next page.

Overview

When the server connects to another server, such as the OpenText Enterprise Performance Engineering server, that requires a secure connection, you must configure trust on the OpenText Application Quality Management server to the authority that issued the remote server certificate.

For more secure communication with the OpenText Application Quality Management server, you can configure Jetty to use TLS 1.3.

When enabling a secure connection, you should also ensure encrypted communication with cookies by setting a site configuration parameter.

Configure trust on the server

Configure trust on the server, when it connects to another server over a secure connection.

1. Obtain the certificate of the root and any intermediate Certificate Authority that issued the remote server certificate.
2. On the server, go to the java bin. For example:

   ```
   C:\Program Files\Java\jre\bin
   ```

3. Import each certificate into the java truststore by using a keytool command. For example:

```
C:\Program Files\Java\jre\bin\keytool -import -trustcacerts
-alias myCA -file <path to certificate> -keystore
"c:\Program Files\java\jre\lib\security\cacerts"
```

4. If your access is denied, run CMD as an administrator.

Configure a secure connection to the application server (Jetty)

1. Obtain the server certificate issued to the name of this server in java keystore format. It must contain a private key and the certificate authority that issued it. For details on creating certificates using the Certificate Authority, see this KB article.
2. Verify that all users have logged out of projects and stop the service.
3. Navigate to the **<Deployment folder>\server\conf** directory. Make a backup of the **jetty.properties** file and the **keystore** file located in this directory.
4. Copy your keystore file to this directory and rename it **keystore**.
5. (Optional) To change the Jetty port, open the **jetty-ssl.xml** file.

```
<Set name="port"><Property name="jetty.ssl.port" default="<your port>"></Set>
```

6. To change keystore related settings, such as passwords and keystore file path, open the **jetty.properties** file.

```
#ssl
jetty.sslContext.keyStorePassword=<your password>
jetty.sslContext.trustStorePassword=<your password>
jetty.sslContext.KeyManagerPassword=<your password>
jetty.sslContext.trustStorePath=<your path>
jetty.sslContext.KeyStorePath=<your path>
```

7. (Strongly recommended) To obfuscate the passwords, perform the following steps:
   a. Determine the version of Jetty that you are using. Locate the **<Deployment folder>\server\lib\jetty-util-<your-jetty-version>.jar** file. **<your-jetty-version>** is the version of Jetty you are using.
   b. Open Command Prompt (cmd) and run the following commands:

```
$ set JETTY_VERSION=<your-jetty-version>
<JAVA_HOME>\java -cp <Deployment folder>\server\lib\jetty-util-$JETTY_
VERSION.jar
org.eclipse.jetty.util.security.Password <password>
```

   For example, if you run the following command:

```
"C:\Program Files\java\jre\bin\java.exe" -cp <Deployment
folder>\server\lib\jetty-util-9.1.4.v20140401.jar
org.eclipse.jetty.util.security.Password changeit
```

   The output will appear as follows:

```
changeit
OBF:1vn21ugu1saj1v9i1v941sar1ugw1vo0
```

   c. Replace the plain text password in the **jetty.properties** file with the **OBF** prefix.
   d. Save the **jetty.properties** file.
8. Open the **start.ini** file, uncomment the following lines, and save the file.

```
jetty-ssl.xml
jetty-ssl-context.xml
```

9. Restart the service.
10. Check the **wrapper.log** file. If you do not see the "Server is ready!" message, correct the errors shown in the log.

11. Connect to OpenText Application Quality Management using the SSL connection, such as **https://<server>:8443/qcbin**.
12. After ensuring that the SSL connection works, disable non-HTTPS access to the application server.
    a. In the **jetty.xml** file, locate the following section and comment it out by placing **<!--** at the beginning of the section, and **-->** at the end.

> **Note:** It is possible that this section in your **jetty.xml** file is

slightly different.

```
<!--
<Call name="addConnector">
    <Arg>
         <New class="org.eclipse.jetty.server.ServerConnector">
          <Arg name="server"><Ref refid="Server" /></Arg>
          <Arg name="factories">
            <Array type="org.eclipse.jetty.server.ConnectionFactory">
                  <Item>
                 <New
class="org.eclipse.jetty.server.HttpConnectionFactory">
                <Arg name="config"><Ref refid="httpConfig" /></Arg>
                </New>
              </Item>
            </Array>
          </Arg>
           <Set name="host"><Property name="jetty.host" /></Set>
           <Set name="port"><Property name="jetty.port"
default="8080"/></Set>
           <Set name="idleTimeout"><Property name="http.timeout"
default="30000"/></Set>
        </New>
      </Arg>
</Call>
-->
```

b. Save the **jetty.xml** file.

13. Restart the ALM service and ensure that the non-secure URL (such as **http://<ALM server>:8080/qcbin**) does not open.

Use TLS 1.3 or TLS 1.2 for secure connection

Use TLS 1.3 or 1.2 for secure connection with the application server and the database server.

> **Note:**
>
> - Oracle databases certified by OpenText Application Quality Management do not support TLS 1.3.
> - Use of the TLS 1.1, TLS 1.0, and SSL 3 protocols is deprecated. OpenText recommends that you do not use them.

Use TLS 1.3 or 1.2 for secure connection with the application server

To use TLS 1.3 or 1.2 for secure connection with the server, configure the **jetty-ssl-context.xml** file as follows:

1. **Prerequisite:** JDK/JRE 17.
2. Verify that all users have logged out of projects and stop the service.
3. Navigate to the **<Deployment folder>\server\conf** directory and make a backup of the **jetty-ssl-context.xml** file.
4. Open the **jetty-ssl-context.xml** file.
5. Uncomment the **ExcludeProtocols** section in the file:

```
<Set name="ExcludeProtocols">
      <Array type="java.lang.String">
            <Item>SSLv3</Item>
            <Item>TLSv1</Item>
            <Item>TLSv1.1</Item>
      </Array>
</Set>
```

> **Note:** You can choose your own set of supported protocols by adding or removing items in this list.
>
> For example, if you want to use TLS 1.3 only, also add TLS 1.2 in the list.

6. Save the **jetty-ssl-context.xml** file.
7. Start the service.

Use TLS 1.3 or 1.2 for secure connection with the database server

- To use TLS 1.3:
  a. **Prerequisite:** Make sure you use SQL Server 2022, with the hotfix for the Bug 2042238 applied.

  > **About the hotfix for the Bug 2042238:** It fixes the following error error that occurs when using the strict encryption option in your connection settings.
  >
  > "The incoming tabular data stream (TDS) remote procedure call (RPC) protocol stream is incorrect. Parameter 1 (""): Data type 0x00 is unknown"
  >
  > For details, see the Microsoft documentation.

  b. Modify the database connection string by adding **Encrypt=strict** to the JDBC connection string. For example:

  jdbc:sqlserver://<your server name>:<port>;EncryptionMethod=SSL;Encrypt=strict

- To use TLS 1.2 for secure connection with the database server, modify the database connection string by adding **CryptoProtocolVersion=TLSv1.2** to the JDBC connection string. For example:

  jdbc:sqlserver://<your server name>:<port>;EncryptionMethod=SSL;CryptoProtocolVersion=TLSv1.2

For details about changing connection string, see the Site Administration help.

For Oracle databases: Place the Oracle Wallet file in a location on the ALM server where the ALM Service user has read permissions.

Redirect http to https

This procedure describes how to redirect http to https. You need to redirect to https when accessing the server directly, and not through a front-end server.

1. Edit **<Deployment folder>\webapps\qcbin\WEB-INF\web.xml**, and add the following at the end (before </web-app>):

```
<security-constraint>
        <web-resource-collection>
                <web-resource-name>Everything</web-resource-name>
                <url-pattern>/*</url-pattern>
        </web-resource-collection>
        <user-data-constraint>
                <transport-guarantee>CONFIDENTIAL</transport-guarantee>
        </user-data-constraint>
</security-constraint>
```

2. Restart OpenText Application Quality Management.
3. Access the system via **http://<server>:8080/qcbin**.

   You should be redirected to **https://<server>:8443/qcbin**. If not, ensure that **SecurePort** in **jetty.xml** matches your secure port.

Set up encrypted communication with cookies

1. In Site Administration, click the **Configuration** tab.
2. click the **Add New Parameter** button. Enter the following information:

Parameter	Value
SSO_SECURE_ONLY_COOKIE	Y

Configure secure access on Linux systems

This topic describes how to configure a secure connection to and from OpenText Application Quality Management when it is installed on a Linux system. For the procedure, see "Configure a secure connection to the application server (Jetty)" on the next page.

Overview

When the OpenText Application Quality Management server connects to another server, such as the OpenText Enterprise Performance Engineering server, that requires a secure connection, you must configure trust on the OpenText Application Quality Management server to the authority that issued the remote server certificate.

For more secure communication with the OpenText Application Quality Management server, you can configure Jetty to use TLS 1.2.

When enabling a secure connection, you should also ensure encrypted communication with cookies by setting a site configuration parameter.

Configure trust on the server

Configure trust on the server, when it connects to another server over a secure connection.

1. Obtain the certificate of the root and any intermediate Certificate Authority that issued the remote server certificate.
2. On the server, go to the java bin. For example:

   ```
   /usr/java/jre/bin
   ```

3. Import each certificate into the java truststore by using a keytool command. For example:

```
 /usr/java/jre/bin/keytool -import -trustcacerts -alias myCA
-file <path to certificate> -keystore
"/usr/java/jre/lib/security/cacerts"
```

Configure a secure connection to the application server (Jetty)

1. Obtain the server certificate issued to the name of this server in java keystore format. It must contain a private key and the certificate authority that issued it. For details on creating certificates using the Certificate Authority, see this KB article.
2. Verify that all users have logged out of projects, and stop the service.
3. Navigate to the **<Deployment folder>/server/conf** directory. Make a backup of the **jetty.properties** file and the **keystore** file located in this directory.
4. (Optional) To change the Jetty port, open the **jetty-ssl.xml** file.

```
<Set name="port"><Property name="jetty.ssl.port" default="<your port>"></Set>
```

5. To change keystore related settings, such as passwords and keystore file path, open the **jetty.properties** file.

```
#ssl
jetty.sslContext.keyStorePassword=<your password>
jetty.sslContext.trustStorePassword=<your password>
jetty.sslContext.KeyManagerPassword=<your password>
jetty.sslContext.trustStorePath=<your path>
jetty.sslContext.KeyStorePath=<your path>
```

6. (Strongly recommended) To obfuscate the password, perform the following steps:
   a. Determine the version of Jetty that you are using. Locate the **<Deployment folder>/server/lib/jetty-util-<your-jetty-version>.jar** file. **<your-jetty-version>** is the version of Jetty you are using.
   b. Open Shell Prompt and run the following commands:

```
$ export JETTY_VERSION=<your-jetty-version>
<JAVA_HOME>/java -cp <installdir>/server/lib/jetty-util-
$JETTY_VERSION.jar
org.eclipse.jetty.util.security.Password <password>
```

   For example, if you run the following command:

```
<JAVA_HOME>/java -cp <ALM deployment
path>/server/lib/jetty-util-9.1.4.v20140401.jar
org.eclipse.jetty.util.security.Password changeit
```

   The output will appear as follows:

```
changeit
OBF:1vn21ugu1saj1v9i1v941sar1ugw1vo0
```

   c. Replace the plain text password in the **jetty.properties**file with the **OBF** prefix.
   d. Save the **jetty.properties**file.
7. Open the **start.ini** file, uncomment the following lines, and save the file.

```
jetty-ssl.xml
jetty-ssl-context.xml
```

8. Restart the service.

9. Check the **wrapper.log** file. If you do not see the "Server is ready!" message, correct the errors shown in the log.
10. Connect to OpenText Application Quality Management using using the SSL connection.
11. After ensuring that the SSL connection works, disable non-HTTPS access to the application server.
    a. In the **jetty.xml** file, locate the following section and comment it out by placing **<!--** at the beginning of the section, and **-->** at the end.

```
<!--
<Call name="addConnector">
    <Arg>
        <New class="org.eclipse.jetty.server.ServerConnector">
            <Arg name="server"><Ref refid="Server" /></Arg>
            <Arg name="factories">
                <Array type="org.eclipse.jetty.server.ConnectionFactory">
                    <Item>
                        <New class="org.eclipse.jetty.server.HttpConnectionFactory">
                            <Arg name="config"><Ref refid="httpConfig" /></Arg>
                        </New>
                    </Item>
                </Array>
            </Arg>
                <Set name="host"><Property name="jetty.host" /></Set>
                <Set name="port"><Property name="jetty.port" default="8080"/></Set>
                <Set name="idleTimeout"><Property name="http.timeout"
default="30000"/></Set>
        </New>
    </Arg>
</Call>
-->
```

> **Note:** It is possible that this section in your **jetty.xml** file is slightly different.

    b. Save the **jetty.xml** file.
12. Restart the service and ensure that the non-secure URL does not open.

Use TLS 1.3 or TLS 1.2 for secure connection

Use TLS 1.3 or 1.2 for secure connection with the application server and the database server.

> **Note:**
>
> - Oracle databases certified by OpenText Application Quality Management do not support TLS 1.3.
> - Use of the TLS 1.1, TLS 1.0, and SSL 3 protocols is deprecated. It's recommended you do not use them.

Use TLS 1.3 for secure connection with the server

To use TLS 1.3 or 1.2 for secure connection with the server, configure the **jetty-ssl-context.xml** file as follows:

1. **Prerequisite:** JDK/JRE 17.
2. Navigate to the **<Deployment folder>/server/conf** directory and make a backup of the **jetty-ssl-context.xml** file.
3. Open the **jetty-ssl-context.xml** file.
4. Uncomment the **ExcludeProtocols** section in the file:

```
<Set name="ExcludeProtocols">
      <Array type="java.lang.String">
            <Item>SSLv3</Item>
            <Item>TLSv1</Item>
            <Item>TLSv1.1</Item>
      </Array>
</Set>
```

> **Note:** You can choose your own set of supported protocols by adding or removing items in this list.

> For example, if you want to use TLS 1.3 only, also add TLS 1.2 in the list.

5. Save the **jetty-ssl-context.xml** file.
6. Start the service.

Use TLS 1.3 or 1.2 for secure connection with the database

- To use TLS 1.3:
  a. **Prerequisite:** Make sure you use SQL Server 2022, with the hotfix for the Bug 2042238 applied.

  > **About the hotfix for the Bug 2042238:** It fixes the following error error that occurs when using the strict encryption option in your connection settings.
  >
  > "The incoming tabular data stream (TDS) remote procedure call (RPC) protocol stream is incorrect. Parameter 1 (""): Data type 0x00 is unknown"
  >
  > For details, see the Microsoft documentation.

  b. Modify the database connection string by adding **Encrypt=strict** to the JDBC connection string. For example:

  jdbc:sqlserver://<your server name>:<port>;EncryptionMethod=SSL;Encrypt=strict

- To use TLS 1.2 for secure connection with the database, modify the database connection string by adding **CryptoProtocolVersion=TLSv1.2** to the JDBC connection string. For example:

  jdbc:sqlserver://<your server name>:<port>;EncryptionMethod=SSL;CryptoProtocolVersion=TLSv1.2

  For details about changing connection string, see the Site Administration help.

For Oracle databases: Place the Oracle Wallet file in a location on the ALM server where the ALM Service user has read permissions.

Redirect http to https

This procedure describes how to redirect http to https. You need to redirect to https when accessing the ALM server directly, and not through a front-end server.

1. Edit **<Deployment folder>/webapps/qcbin/WEB-INF/web.xml**, and add the following at the end (before </web-app>):

```
<security-constraint>
        <web-resource-collection>
                <web-resource-name>Everything</web-resource-name>
                <url-pattern>/*</url-pattern>
        </web-resource-collection>
        <user-data-constraint>
                <transport-guarantee>CONFIDENTIAL</transport-guarantee>
        </user-data-constraint>
</security-constraint>
```

2. Restart OpenText Application Quality Management.
3. Access the system via **http://<server>:8080/qcbin**.

   You should be redirected to **https://<server>:8443/qcbin**. If not, ensure that **SecurePort** in **jetty.xml** matches your secure port.

Set up encrypted communication with cookies

1. In Site Administration, click the **Site Configuration** tab.
2. click the **New Parameter** button. Enter the following information:

Parameter	Value
SSO_SECURE_ONLY_COOKIE	Y

Configuring secure database access

This topic describes how to configure a secure connection, such as Secure Socket Layer (SSL), from the OpenText Application Quality Management server to the database server. If your database server requires an encrypted channel, you must follow these instructions.

Before you start

Before beginning, determine the following:

Database	Considerations
SQL	• Is the certificate signed by a trusted Certificate Authority (CA)? If not, obtain the certificate chain of authority that issued your SQL server certificate and import it into the ALM server truststore using the procedure to configure trust on the ALM server in "Configure secure access on Windows systems" on page 141 or "Configure secure access on Linux systems" on page 149. • Is host name validation required? If yes, what is the host name, including the domain name, in the server certificate?
Oracle	If the database is SSL configured: • Place the Oracle Wallet file in a location on the ALM server where the ALM Service user has read permissions. • Is host name validation required? If yes, what is the host name, including the domain name, in the server certificate? • Is the port different than what it was before? If the database is not SSL configured: • Is native Data Integrity configured? • Is native Encryption configured? If yes, what is the algorithm? Is the key larger than 128 bits?

Configure a secure connection for a previously unsecured database.

To configure a secure database connection for a previously unsecured database:

1. For SQL databases, follow the procedure to configure trust on the ALM server in "Configure secure access on Windows systems" on page 141 or "Configure secure access on Linux systems" on page 149.
2. Configure the Site Administration schema connection.

This section is relevant if the database server that was configured for a secure connection contains your Site Administration schema. If you have a separate database server for your projects and you only want a secure connection to that database, skip this section.

OS	Steps

Windows	a. Stop the server.
	b. Run the Server Configuration wizard:
	`Win > Run > "%ALM_INSTALL_PATH%\run_configuration.bat" gui false`
	c. In the Database Server step, enter the database administrator password and click **Next**.
	d. Select the **Connection String** option under **Database Connection**:
	◦ For SSL, add **;encrypt=true** to the end of the value. For example:
	`jdbc:sqlserver://localhost:1433;databaseName=DBNAME;integratedSecurity=true;encrypt=true;trustServerCertificate=true`
	◦ For Oracle, add **;javax.net.ssl.trustStore=[path to Oracle Wallet];javax.net.ssl.trustStorePassword=[password to Oracle wallet]** to the end of the value. For example:
	`jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=servername)(PORT=2484))(CONNECT_DATA=(SERVICE_NAME=servicename)));javax.net.ssl.trustStore=C:\path\ewallet.p12;javax.net.ssl.trustStorePassword=password;javax.net.ssl.trustStoreType=PKCS12`
	Alternatively, you can import the certificate as a Java keystore (.jks) file into the Java cacerts store.
	For details about how to enable providers in java security files, see the Oracle JDBC driver documentation.
	◦ For Oracle native Data Integrity, add **;oracle.net.crypto_checksum_client =ACCEPTED** or **;oracle.net.crypto_checksum_client =REQUIRED** to the end of the value, and replace the java security policy files in `..\java\jre\lib\security\`.
	◦ For Oracle native Encryption, add **;oracle.net.crypto_**

OS	Steps
	checksum_client =ACCEPTED or **;oracle.net.crypto_ checksum_client =REQUIRED** to the end of the value, and, for encryption algorithms with keys longer than 128 bits, replace the java security policy files in `..\java\jre\lib\security\`. **Note:** For details on java security policy files, see the Oracle documentation. e. Click **Next**. In the Site Administration Database Schema step: i. Select **Connect to existing schema/ second node** under **Selected Action**. ii. Enter your Site Administration schema name and password. f. Continue until the end of the wizard and start the ALM Service.

OS	Steps

Linux	a. Stop the OpenText Application Quality Management server.
	b. Edit the **qcConfigFile.properties** file located in the deployment folder.
	i. Value SaDbAction with connectToExisting
	`SaDbAction=connectToExisting`
	ii. Edit the line with dbConnectionString:
	• For SSL, add **;encrypt=true** to the end of the value. For example:
	`jdbc:sqlserver://localhost:1433;databaseName=DBNAME;integratedSecurity=true;encrypt=true;trustServerCertificate=true`
	• For Oracle, add **;javax.net.ssl.trustStore=[path to Oracle Wallet];javax.net.ssl.trustStorePassword=[password to Oracle wallet]** to the end of the value. For example:
	`jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=servername)(PORT=2484))(CONNECT_DATA=(SERVICE_NAME=servicename)));javax.net.ssl.trustStore=/path/ewallet.p12;javax.net.ssl.trustStorePassword=password;javax.net.ssl.trustStoreType=PKCS12`
	Alternatively, you can import the certificate as a Java keystore (.jks) file into the Java cacerts store.
	• For Oracle native Data Integrity, add **;oracle.net.crypto_checksum_client =ACCEPTED** or **;oracle.net.crypto_checksum_client =REQUIRED** to the end of the value, and replace the java security policy files in `../java/jre/lib/security/`.
	• For Oracle native Encryption, add **;oracle.net.crypto_checksum_client =ACCEPTED** or **;oracle.net.crypto_checksum_client =REQUIRED** to the end of the value, and, for encryption algorithms with keys longer than 128

OS	Steps
	bits, replace the java security policy files in `../java/jre/lib/security/`. **Note:** For details on java security policy files, see the Oracle documentation. c. Run the Server Configuration wizard from the ALM installation folder: `./run_configuration.sh` d. Wait until the server is reconfigured and start the ALM Service.

3. Configure the database servers:
   a. Log in to Site Administration.
   b. In the Database Servers tab, do the following for each database that was configured for a secure connection:
      i. Select the database and click **Edit**.
      ii. Change the connection string:
      - For SSL, add **;encrypt=true** to the end of the value.
      - For Oracle, add **;javax.net.ssl.trustStore=[path to Oracle Wallet];javax.net.ssl.trustStorePassword=[password to Oracle wallet]** to the end of the value.
      - For Oracle native Data Integrity, add **;oracle.net.crypto_checksum_client =ACCEPTED** or **;oracle.net.crypto_checksum_client =REQUIRED** to the end of the value, and replace the java security policy files in `..\java\jre\lib\security\`.
      - For Oracle native Encryption, add **;oracle.net.crypto_checksum_client =ACCEPTED** or **;oracle.net.crypto_checksum_client =REQUIRED** to the end of the value, and, for encryption algorithms with keys longer than 128 bits, replace the java security policy files in `..\java\jre\lib\security\`.

> **Note:** For details on java security policy files, see the Oracle documentation.

iii. Click **Test Connection** to check that the connection works.

iv. Click **OK**.

4. Configure LAB_PROJECT, if LAB_PROJECT is on a secure connection database:

   a. Log in to Site Administration.

   b. Go to the Site Projects tab, select LAB_PROJECT, and click **Edit** :

      i. Click **OK** for any error messages that appear.

      ii. The Connection String Editor (MS-SQL/Oracle) dialog box opens. Change the connection string:

      - For SSL, add **;encrypt=true** to the end of the value.
      - For Oracle, add **;javax.net.ssl.trustStore=[path to Oracle Wallet];javax.net.ssl.trustStorePassword=[password to Oracle wallet]** to the end of the value.
      - For Oracle native Data Integrity, add **;oracle.net.crypto_checksum_client =ACCEPTED** or **;oracle.net.crypto_checksum_client =REQUIRED** to the end of the value, and replace the java security policy files in `..\java\jre\lib\security\`.
      - For Oracle native Encryption, add **;oracle.net.crypto_checksum_client =ACCEPTED** or **;oracle.net.crypto_checksum_client =REQUIRED** to the end of the value, and, for encryption algorithms with keys longer than 128 bits, replace the java security policy files in `..\java\jre\lib\security\`.

> **Note:** For details on java security policy files, see the Oracle documentation.

iii. Click **Test Connection** to check that the connection works.

iv. Click **OK**.

v. Click **Activate Project**.

5. Configure all site projects on a secure connection database:

   a. Log in to Site Administration.

   b. Go to the Site Projects tab, select the project and click **Edit**:

      i. Click **OK** for any error messages that appear.

      ii. The Connection String Editor (MS-SQL/Oracle) dialog box opens. Change the connection string:

      - For SSL, add **;encrypt=true** to the end of the value.
      - For Oracle, add **;javax.net.ssl.trustStore=[path to Oracle Wallet];javax.net.ssl.trustStorePassword=[password to Oracle wallet]** to the end of the value.
      - For Oracle native Data Integrity, add **;oracle.net.crypto_checksum_client =ACCEPTED** or **;oracle.net.crypto_checksum_client =REQUIRED** to the end of the value, and replace the java security policy files in `..\java\jre\lib\security\`.
      - For Oracle native Encryption, add **;oracle.net.crypto_checksum_client =ACCEPTED** or **;oracle.net.crypto_checksum_client =REQUIRED** to the end of the value, and, for encryption algorithms with keys longer than 128 bits, replace the java security policy files in `..\java\jre\lib\security\`.

      > **Note:** For details on java security policy files, see the Oracle documentation.

      iii. Click **Test Connection** to check that the connection works.

      iv. Click **OK**.

      v. Click **Activate Project**.

c. Perform the above step for all projects on a secure connection database.

   If you have a large number of projects to update, you can run the following SQL update query on the site administration schema:

   i. In MS SQL Server: UPDATE td.PROJECTS SET DB_CONNSTR_FORMAT = 'your new connection string'

   ii. In Oracle: UPDATE [your sa schema name].PROJECTS SET DB_CONNSTR_FORMAT = 'your new connection string'

   iii. To limit the projects you update, add a where clause to the query, such as WHERE PROJECT_NAME IN ('project1', 'project2') or WHERE DOMAIN_NAME IN ('damain1', 'domain2')

   iv. After executing the query, restart the ALM service.

Configure a secure database connection for a new installation

You can configure a secure database connection for a new installation as follows:

1. For SQL databases, follow the procedure to configure trust on the ALM server in "Configure secure access on Windows systems" on page 141 or "Configure secure access on Linux systems" on page 149.
2. During the installing, in the Database Server step, select the Connection String option and value the field as follows:
   - For MS SQL server use this format: **jdbc:sqlserver://;serverName:1433;encrypt=true;**.

     If TLSv1.2 is required use this format: **jdbc:sqlserver://;serverName:1433;encrypt=true; sslProtocol=TLSv1.2;**.
   - For Oracle, add **;javax.net.ssl.trustStore=[path to Oracle Wallet];javax.net.ssl.trustStorePassword=[password to Oracle wallet]** to the end of the value.

For details, see the Oracle JDBC driver documentation.

- For Oracle native Data Integrity, add **;oracle.net.crypto_checksum_client =ACCEPTED** or **;oracle.net.crypto_checksum_client =REQUIRED** to the end of the value, and replace the java security policy files in `..\java\jre\lib\security\`.
- For Oracle native Encryption, add **;oracle.net.crypto_checksum_client =ACCEPTED** or **;oracle.net.crypto_checksum_client =REQUIRED** to the end of the value, and, for encryption algorithms with keys longer than 128 bits, replace the java security policy files in `..\java\jre\lib\security\`.

> **Note:** For details on java security policy files, see the Oracle documentation.

3. Complete the installation.

Customize system files

You can customize various aspects of OpenText Application Quality Management by creating or configuring system files.

This section includes:

Customize Site Administration

Customization of the Site Administration repository and the **qcbin** application, such as editing **.xsl** mail stylesheets or creating custom test types, must be performed in the deployment directory. After customizing any of the files in

the deployment directory, you must redeploy OpenText Application Quality Management.

> **Caution:** You must not modify, add, or delete files in the ALM installation directory.

Customize the Site Administration Repository

Perform the following procedure to customize the Site Administration repository.

1. On the machine on which OpenText Application Quality Management is installed, open a file browser, and navigate to **<Installation path>\ALM\data\sa**.
2. Open another file browser, and navigate to **<Repository path>\customerData**.
3. In the installation directory, navigate to the file that you want to customize.
4. In the repository directory, under **customerData**, create the same folder structure that contains the file in the installation directory.
5. Copy the file from the installation directory and paste the file in the appropriate folder in the repository directory.
6. Edit the file in the repository directory.
7. Run the Server Deployment Wizard.

OS	Details
Windows	**Start > OpenText ALM Server > Server Deployment Wizard** or **<installation path>\bin\run_server_deploy_tool.bat**
Linux	**<installation path>/bin/run_server_deploy_tool.sh**

Customize the qcbin Application

Perform the following procedure to customize the qcbin application.

1. On the machine on which OpenText Application Quality Management is installed, open a file browser, and navigate to **<Installation path>\ALM\application\20qcbin.war**.
2. Open another file browser, and navigate to **<Deployment path>\application\20qcbin.war**.
3. In the installation directory, navigate to the file that you want to customize.
4. In the deployment directory, under **20qcbin.war** create the same folder structure that contains the file in the installation directory.
5. Copy the file from the installation directory and paste the file in the appropriate folder in the deployment directory.
6. Edit the file in the deployment directory.
7. Run the Server Deployment Wizard from

OS	Details
Windows	**Start > OpenText ALM Server > Server Deployment Wizard** or **<installation path>\bin\run_server_deploy_tool.bat**
Linux	**<installation path>/bin/run_server_deploy_tool.sh**

8. Repeat the procedure on each cluster node.

Customize menus

You can customize the Tools and Help menus by modifying the **ALM-Client.exe.config** file on the machine on which OpenText Application Quality Management is installed.

> **Note:** You can only perform **.cab** related actions on a Windows machine. To customize menus, copy the relevant files to a Windows machine and edit the files as necessary. Then copy the files back to the machine on which OpenText Application Quality Management is installed and proceed as instructed.

To customize OpenText Application Quality Management:

1. On the machine on which OpenText Application Quality Management is installed, extract the **ALM-Client.exe.config** file from **Client.cab**. This file is located in: **<ALM deployment path>\deployment\20qcbin.war\Install**.
2. Open the **ALM-Client.exe.config** file (this is in **.xml** format).
3. In the **Tools** section of the file, you can add new items to the Tools menu.

   The following is the syntax of an entry in the **Tools** line:

   ```
   <TDFrame
           Tools="<Tool_Name>,{<Tool_ID>}"
           Workflow="{<Workflow_ID>}"
           Parameters="<parameters>"
   />
   ```

4. To change, delete, or rearrange the list of items in the Help menu, change the default names, IDs, and URLs listed in the **OnlineHelpItem** line. The following is the syntax of an entry in the **OnlineHelpItem** line:

   ```
   <OnlineHelpItem
   ID="<Help_ID>"
   Name="<Help_Name>"
   Url="<Help_URL>"
   ```

   To create a separator line between two items in the Help menu, use the following syntax:

   ```
   <OnlineHelpItem
   ID="<Help_ID>"
   Name="<Help_Name>"
   Url="<Help_URL>"
   ```

```
IsFirstInGroup="true" />
```

> **Note:** The first two menu items in the Help menu, **Help on this page** and **ALM Help**, and the last Help menu item, **About OpenText Application Quality Management Software**, cannot be moved or changed. They do not have corresponding entries in the **QualityCenter.exe.config** file. The above step only affects the menu items between them.

5. Unzip the **Client.cab** file to a temporary folder named **Client** which must be under the temp folder. For example, C:\temp\Client.
6. Replace the **ALM-Client.exe.config** file with the modified file.
7. Store the temporary folder on a logical drive, for example X, by running the following command:

   ```
   subst [X]: <temp folder>
   ```

   For example: **subst X: C:\temp**
8. Create a new **Client.cab** file with the following command:

   ```
   cabarc -r -p -P Client\ -s 6144 N <temp folder>\Client.cab
   X:\Client\*.*
   ```

   > **Note:** To use this command you must first download cabsdk.exe (the Cabinet Software Development Kit) from the Microsoft Download Center.
9. Add a class 3 digital signature to the new **Client.cab** file.

   > **Note:** The digital signature must be a signature of a trusted provider.
10. Under **<Deployment path>\application\20qcbin.war**, create a new Installation folder, if it does not already exist.
11. Save the new cab file under the Installation folder.

12. Run the Server Deployment Wizard

OS	Details
Windows	**Start > OpenText ALM Server > Server Deployment Wizard** or **<installation path>\bin\run_server_deploy_tool.bat**
Linux	**<installation path>/bin/run_server_deploy_tool.sh**

13. Repeat the procedure on each cluster node.

Customize the system tray icon

> **Note:** This section applies to Windows systems only.

The system tray icon indicates the current status of OpenText Application Quality Management. It also indicates the current action that OpenText Application Quality Management is performing.

You can customize the behavior of the icon by modifying the **trayConfigFile.properties** file.

To customize the system tray icon:

1. Navigate to the following directory: **<Deployment folder>\server\conf**
2. Open the **trayConfigFile.properties** file.
3. Change the following properties as necessary:
   - **pollingintervalMillis.** Defines, in milliseconds, how often the ALM system tray icon checks the status (started or stopped) of ALM. The default value is 5,000.
   - **logDebugMode.** Defines whether debugging information is included in the system tray log. The default value is false.
   - **timeoutintervalMillis.** Defines, in milliseconds, the maximum amount of time ALM takes to change the status of ALM when you right-click the icon and choose Start/Stop ALM Server. If ALM is not able to perform

the action in the allotted time the status changes to Error. The default value is 180,000.

> **Note:** If the icon does not appear in the system tray, choose **Start > Programs > OpenText Application Quality Management > OpenText Application Quality Management Tray icon**.

Customize the login window

You can customize the login window, so that you can share any special announcements or important events with users that are using the same ALM server. When working in Windows, you can also replace the existing background photo displayed in the ALM Login window. Users can view these changes from their ALM Desktop Client machines.

Display a message in the Login window

This section describes how to display a message in the Login window.

1. On the server, navigate to the following directory:

Windows	`<Deployment path>\webapps\qcbin\Help\` (**By default:** `C:\ProgramData\HP\ALM\webapps\qcbin\Help\`)
Linux	`<Deployment path>/webapps/qcbin/Help/` (**By default:** `/var/opt/ALM/webapps/qcbin/Help/`)

2. Create the **customization** folder.
3. In the customization folder, create the following file: **customizationInfo.htm**. The file name is case-sensitive.
4. Edit the **customizationInfo.htm** file and add content.
5. To view the content, open the Login window from the ALM Desktop Client machine.

Customize the background photo in the Login window

This section describes how to replace the background photo displayed in the Login window.

> **Note:**
> - We recommend using a square-shaped photo. The minimum is 900 pixels wide by 900 pixels height.
> - If it takes too long for the customized background photo to download, then the default background is displayed.

1. On the server, navigate to the following directory:

Windows	`<Deployment path>\webapps\qcbin\images` (**By default:** `C:\ProgramData\HP\ALM\webapps\qcbin\images`)
Linux	`<Deployment path>/webapps/qcbin/images` (**By default:** `/var/opt/ALM/webapps/qcbin/images`)

2. Copy the customized background picture to this folder and rename it to **login-bg-cust.jpg**. The file name is case-sensitive.

Uninstall

You can uninstall OpenText Application Quality Management from the server machine. When uninstalling OpenText Application Quality Management, projects are not deleted. You can also uninstall OpenText Application Quality Management client components from a client machine that has been used to access OpenText Application Quality Management.

Uninstall from Windows systems

This section describes how to uninstall ALM from your Windows server machine.

- Select **Start > All Programs > OpenText Application Quality Management**. Run **Uninstall OpenText Application Quality Management**.

  Alternatively, navigate to the installation directory (the default is **C:\Program Files\Micro Focus\ALM\ALM**). Run the **Uninstall_ALM.exe** file.
- (Optional) To remove all traces of OpenText Application Quality Management from the machine, delete all remaining files in the installation directory as well as the deployment path. Also delete the **\..\ALM** folders in the **c:\ProgramData** directory and their files

> **Note:** When you remove the repository directory, all projects' repositories are also removed. The database remains unless it is specifically deleted.

Uninstall from Linux systems

This section describes how to uninstall OpenText Application Quality Management from your Linux server machine.

> **Note:** You must log on to the server machine as the same user that installed OpenText Application Quality Management.

1. Navigate to the installation directory (the default is **/root/ALM/ALM**).
2. Run the **Uninstall_ALM** file (./Uninstall_ALM).
3. (Optional) To remove all traces of OpenText Application Quality Management from the machine, delete all remaining files in the installation directory as well as the deployment path. Also delete the **/OpenText/ALM** folders in the **/var/opt** directory and their files.

   > **Note:** When you remove the repository directory, all projects' repositories are also removed. The database remains unless it is specifically deleted.

Remove client components from a client machine

When you run OpenText Application Quality Management on your client computer, client components are downloaded to your client machine. You can use the ALM Client Cleanup add-in to remove all ALM client components, including files and registry keys. For details and to download the add-in, see the ALM Client Cleanup Add-in page on Marketplace.

If the client machine is used to access OpenText Application Quality Management after the cleanup add-in has been run, all necessary components are downloaded again from the OpenText Application Quality Management server.

Project upgrade

You can upgrade projects individually or on the domain level.

Deactivate and remove projects from existing installation

> **Note:** Back up the database and repository after deactivating projects.

In the previous OpenText Application Quality Management/Quality Center installation, deactivate and remove projects from Site Administration. You do not have to deactivate and remove all projects at once. You can perform this action on a per-project upgrade basis.

To deactivate a project:

1. In Site Administration, click the **Projects** tab.
2. In the Projects list, select a project.
3. Click the **Deactivate Project** or **Deactivate Template** button. A message box indicates that all connected users will be disconnected.
4. Click **OK** to confirm. The project is deactivated and the project icon is changed in the Projects list.

To remove a project from the Projects list:

> **Note:** If the project is currently in use, it cannot be removed. For information about how to manually remove a project, see this KB article.

1. In Site Administration, click the **Projects** tab.
2. In the Projects list, select a project.
3. Click the **Remove Project** or **Remove Template** button.
4. Click **OK** to confirm. If the project is still active, you are prompted to

deactivate it.

5. Click **OK**.

Copy project database schemas to the new database server machine

> **Note:** Perform this step only if your new OpenText Application Quality Management system uses a new database server or new instance of the previous database server.

To restore removed projects in the new database server machine, copy the project schemas from the database server that was used in the previous system to the database server that will be used in the new system.

This enables you to restore the projects in Site Administration in the new installation.

Perform the required steps for backing up, removing, and restoring databases for your database type. For assistance contact your database administrator.

> **Note:** The database user must have the same permissions as the user installing OpenText Application Quality Management.

Restore projects in new Site Administration database schema

To view projects in Site Administration, on the machine on which the new version of OpenText Application Quality Management has been installed, restore projects you removed above as follows:

Project restore considerations

- Before restoring the project, make sure that the database where the project resides exists in the **Servers** tab in Site Administration on your OpenText

Application Quality Management server. The OpenText Application Quality Management server needs to access the contents of the restored project from the project's database.

- When restoring a project, you should select the **dbid.xml** file located in the project repository. This ensures that the project retains its original ID. If a project does not have its original ID, the following cross project features may not function properly: cross project customization, importing and synchronizing libraries, and cross project graphs.
- If you are restoring your project from a different directory, or if you renamed your schema or restored it to a different database, you must update the **dbid.xml** file accordingly.
- You must first restore and upgrade any template projects before restoring and upgrading other projects. If the template project and its linked projects are in different databases, ensure that the template project's database is accessible when restoring any linked projects.

To restore access to an OpenText Application Quality Management project:

1. Navigate to the project's **dbid.xml** file. The file is located in the project repository's **qc** sub-directory.

   For details on the project structure, refer to the Understanding the Project Structure section in the *the help*.
2. Open the file and update the following values:

> **Note:**
>
> - To identify the values of **DB_CONNSTR_FORMAT** and **DB_USER_PASS**, it is recommended to create a new, empty project in OpenText Application Quality Management Site Administration, open the project's **dbid.xml** file, and copy these values. You can later delete the empty project.
> - Make sure not to change the original value for **PR_SMART_REPOSITORY_ENABLED**.

> - If you are restoring **LAB_PROJECT** or OpenText Enterprise Performance Engineering projects as part of the upgrade process, make sure not to edit the **PROJECT_UID** value. You must restore these projects with their original **PROJECT_UID** value to maintain the links between **LAB_PROJECT** and its associated OpenText Enterprise Performance Engineering projects. This is important for shared data, such as timeslots, runs, and so on.

- **DB_NAME**. Update to the database schema name as it appears in the database server.
- **DB_CONNSTR_FORMAT**. Update to the value of the empty project created in OpenText Application Quality Management. See the note for details.
- **DBSERVER_NAME**. This is the name of the database server as defined in the **DB Servers** tab in Site Administration.
- **DB_USER_PASS**. Update if the encrypted passphrase differs between the previous installation and OpenText Application Quality Management.
- **PHYSICAL_DIRECTORY**. Update to the new location of the project repository. It must contain a backslash (\) at the end of the path.

3. Save the file.
4. In Site Administration, click the **Site Projects** tab.
5. Click the **Restore Project** or **Restore Template** button. The Restore Project dialog box opens.
6. To locate the file that includes the project that you want to restore, click the browse button to the right of the **dbid.xml file location** box. The Open File dialog box opens.
7. Locate the project's **dbid.xml** file.
8. Select the **dbid.xml** file and click **Open**. The Restore Project dialog box opens and displays the database type, name, server, and the directory path of the project.

9. In the **Restore Into Domain** box, select the domain in which you want the restored project to be located.
10. Click **Restore**.
11. If your database server does not have the text search feature enabled, a message box opens. You can enable the text search feature before or after this process completes.
    - Click **Yes** to continue this process. After the process completes, you can enable the text search feature.
    - Click **No** to stop this process. Enable the text search feature and then restart the process.
12. When the restore process completes, click **OK**.
13. Click **Close** to close the Restore Project dialog box and view the restored project in the Projects list.

Upgrade projects

After a project appears in the OpenText Application Quality Management 25.1 Site Administration project list, you can proceed with the actual project upgrade. You can upgrade projects individually or on the domain level, which upgrades all projects contained in the domain. You must first upgrade any template projects before upgrading other projects.

For details on upgrading projects, see "Upgrade projects" on page 185.

Deactivate and remove projects from an existing installation

> **Note:** Back up the database and repository after deactivating projects.

In the previous OpenText Application Quality Management/Quality Center installation, deactivate and remove projects from Site Administration. You do

not have to deactivate and remove all projects at once. You can perform this action on a per-project upgrade basis.

To deactivate a project:

1. In Site Administration, click the **Projects** tab.
2. In the Projects list, select a project.
3. Click the **Deactivate Project** or **Deactivate Template** button. A message box indicates that all connected users will be disconnected.
4. Click **OK** to confirm. The project is deactivated and the project icon is changed in the Projects list.

To remove a project from the Projects list:

> **Note:** If the project is currently in use, it cannot be removed. For information about how to manually remove a project, see this KB article.

1. In Site Administration, click the **Projects** tab.
2. In the Projects list, select a project.
3. Click the **Remove Project** or **Remove Template** button.
4. Click **OK** to confirm. If the project is still active, you are prompted to deactivate it.
5. Click **OK**.

Copy project database schemas to the new database server machine

> **Note:** Perform this step only if your new OpenText Application Quality Management system uses a new database server or new instance of the previous database server.

To restore removed projects in the new database server machine, copy the project schemas from the database server that was used in the previous system to the database server that will be used in the new system.

This enables you to restore the projects in Site Administration in the new installation.

Perform the required steps for backing up, removing, and restoring databases for your database type. For assistance contact your database administrator.

> **Note:** The database user must have the same permissions as the user installing OpenText Application Quality Management.

Restore projects in new site administration database schema

To view projects in Site Administration, on the machine on which the new version of OpenText Application Quality Management has been installed, restore projects you removed above as follows:

Project restore considerations

- Before restoring the project, make sure that the database where the project resides exists in the **Servers** tab in Site Administration on your OpenText Application Quality Management server. The OpenText Application Quality Management server needs to access the contents of the restored project from the project's database.
- When restoring a project, you should select the **dbid.xml** file located in the project repository. This ensures that the project retains its original ID. If a project does not have its original ID, the following cross project features may not function properly: cross project customization, importing and synchronizing libraries, and cross project graphs.
- If you are restoring your project from a different directory, or if you renamed your schema or restored it to a different database, you must update the **dbid.xml** file accordingly.
- You must first restore and upgrade any template projects before restoring and upgrading other projects. If the template project and its linked projects

are in different databases, ensure that the template project's database is accessible when restoring any linked projects.

To restore access to an OpenText Application Quality Management project:

1. Navigate to the project's **dbid.xml** file. The file is located in the project repository's **qc** sub-directory.

   For details on the project structure, refer to the Understanding the Project Structure section in the *the help*.

2. Open the file and update the following values:

   > **Note:**
   > - To identify the values of **DB_CONNSTR_FORMAT** and **DB_USER_PASS**, it is recommended to create a new, empty project in OpenText Application Quality Management Site Administration, open the project's **dbid.xml** file, and copy these values. You can later delete the empty project.
   > - Make sure not to change the original value for **PR_SMART_REPOSITORY_ENABLED**.
   > - If you are restoring **LAB_PROJECT** or OpenText Enterprise Performance Engineering projects as part of the upgrade process, make sure not to edit the **PROJECT_UID** value. You must restore these projects with their original **PROJECT_UID** value to maintain the links between **LAB_PROJECT** and its associated OpenText Enterprise Performance Engineering projects. This is important for shared data, such as timeslots, runs, and so on.

   - **DB_NAME**. Update to the database schema name as it appears in the database server.
   - **DB_CONNSTR_FORMAT**. Update to the value of the empty project created in OpenText Application Quality Management. See the note for details.
   - **DBSERVER_NAME**. This is the name of the database server as defined in the **DB Servers** tab in Site Administration.

- **DB_USER_PASS**. Update if the encrypted passphrase differs between the previous installation and OpenText Application Quality Management.
- **PHYSICAL_DIRECTORY**. Update to the new location of the project repository. It must contain a backslash (\) at the end of the path.

3. Save the file.
4. In Site Administration, click the **Site Projects** tab.
5. Click the **Restore Project** or **Restore Template** button. The Restore Project dialog box opens.
6. To locate the file that includes the project that you want to restore, click the browse button to the right of the **dbid.xml file location** box. The Open File dialog box opens.
7. Locate the project's **dbid.xml** file.
8. Select the **dbid.xml** file and click **Open**. The Restore Project dialog box opens and displays the database type, name, server, and the directory path of the project.
9. In the **Restore Into Domain** box, select the domain in which you want the restored project to be located.
10. Click **Restore**.
11. If your database server does not have the text search feature enabled, a message box opens. You can enable the text search feature before or after this process completes.
    - Click **Yes** to continue this process. After the process completes, you can enable the text search feature.
    - Click **No** to stop this process. Enable the text search feature and then restart the process.
12. When the restore process completes, click **OK**.
13. Click **Close** to close the Restore Project dialog box and view the restored project in the Projects list.

Upgrade projects

After a project appears in the OpenText Application Quality Management 25.1 Site Administration project list, you can proceed with the actual project upgrade. You can upgrade projects individually or on the domain level, which upgrades all projects contained in the domain. You must first upgrade any template projects before upgrading other projects.

About upgrading domains and projects

By default, the upgrade process runs in non-silent mode. When running the process in non-silent mode, OpenText Application Quality Management may pause and prompt you for input when an error occurs. Instead, you can choose to run the process in silent mode. When running the process in silent mode, OpenText Application Quality Management aborts the process without prompting you for input.

After the project has been upgraded, you can no longer use the project with a previous version of OpenText Application Quality Management/Quality Center.

Note:

- During the upgrade process, the project directory must be accessible. For example, if your project directory is located on a file server, ensure that the server is running and accessible.
- During the upgrade process, no database maintenance jobs can be run. Running database maintenance jobs can cause the upgrade to fail and can corrupt projects.
- If a project has extensions enabled, the availability of these extensions on the new server must be verified before upgrading. If any extension is not available on the new server, the upgrade fails.
- You must first upgrade a template project before upgrading any of its linked projects. If the template project and its linked projects are in

different databases, ensure that the template project's database is accessible when updating any linked projects.

- **Version Control:** Version control enabled projects cannot be upgraded while there are checked out entities. All entities must be checked in to the corresponding version of Quality Center or OpenText Application Quality Management. To determine if there are checked out entities, see this KB article.

Upgrade a domain

This section describes how to upgrade all projects in a domain.

To upgrade a domain:

1. In Site Administration, click the **Projects** tab.
2. In the Projects list, select a domain.
3. Click the **Maintain Domain** button and select **Upgrade Domain**. The Upgrade Domain dialog box opens.
4. In the **Upgrade Settings** area, under **Upgrade Mode**, you can select the following options:
   - **Run in Silent Mode.** Runs the process without any user interaction.
   - **Continue to next project if upgrade failed.** Proceeds to the next project if the upgrade process fails. This is the default option.
5. In the **Upgrade Settings** area, under **After the Upgrade**, you can select one of the following options:
   - **Leave all projects deactivated.** Leaves all projects deactivated after the upgrade process completes.
   - **Activate only currently active projects.** Reactivates previously-activated projects after the upgrade process completes. This is the default option.
   - **Activate all projects.** Activates all projects after the upgrade process completes.

6. To view the current version numbers of your projects, select the project names, or click **Select All** to view version numbers for all projects. Click the **Display Versions** button.

   The project version number is displayed in the **Version** column.

7. To upgrade your projects, select the project names, or click **Select All** to verify all projects. Click the **Upgrade Projects** button.

   If a database error occurs while running the process in non-silent mode, a message box opens. Click the **Abort** or **Retry** buttons, based on whether you can correct the problem described in the message box.

   If the upgrade fails, OpenText Application Quality Management displays an error message with reasons for the failure and refers you to the log file. You must restore the backed up projects before you try to upgrade again. For details, see"Restore backed up projects and repositories" on page 68.

8. To pause the upgrade process, click the **Pause** button. To continue, click the **Resume** button.
9. To abort the upgrade process, click the **Abort** button. Click **Yes** to confirm.
10. To save the messages displayed in the Upgrade Results pane in a text file, click the **Export Log** button. In the Export Log to File dialog box, choose a location and type a name for the file. Click **Save**.
11. To clear the messages displayed in the Upgrade Results pane, click the **Clear Log** button.
12. Click **Close** to close the Upgrade Domain dialog box.

Upgrade a project

This section describes how to upgrade a single project.

To upgrade a project:

1. In Site Administration, click the **Projects** tab.
2. In the Projects list, select a project.
3. Click the **Maintain Project** button and select **Upgrade Project**. The Upgrade Project dialog box opens.
4. To run the upgrade process without any user interaction, select **Run in silent mode**.
5. To start the upgrade process, click the **Upgrade Project** button. If the project is active, you are prompted to deactivate it.

   If a database error occurs while running the process in non-silent mode, a message box opens. Click the **Abort** or **Retry** buttons, based on whether you can correct the problem described in the message box.

   If the upgrade fails, OpenText Application Quality Management displays an error message with reasons for the failure and refers you to the log file. You must restore the backed up project before you try to upgrade again. For details, see "Restore backed up projects and repositories" on page 68.
6. To pause the upgrade process, click the **Pause** button. To continue, click the **Resume** button.
7. To abort the upgrade process, click the **Abort** button. Click **Yes** to confirm.
8. To save the messages displayed in the Upgrade Results pane to a text file, click the **Export Log** button. In the Export Log to File dialog box, choose a location and type a name for the file. Click **Save**.
9. To clear the messages displayed in the Upgrade Results pane, click the **Clear Log** button.

10. Click **Close** to close the Upgrade Project dialog box.
11. Reactivate the project.

Upgrade preparation troubleshooting

This section describes schema and database inconsistencies that the verification process detects. It indicates which problems the repair process can fix automatically, and which you should repair manually. Suggested solutions for repairing each issue are provided.

This section includes:

Overview

The verification process, described in "Verify domains and projects" on page 67, detects inconsistencies and indicates which problems the repair process can fix automatically, and which you should repair manually. Suggested solutions for repairing each issue are provided in this appendix.

If an error is displayed during the verification or upgrade process, you can see error descriptions at this KB article.

If a warning is displayed during the verification process, you can use the "Quick Warning Reference" on the next page to locate the corresponding solution for that warning.

Some solutions require that you change the database user schema:

- **Database User Schema.** Database in SQL Server and a user schema in Oracle. This term is used for both cases because OpenText Application Quality Management can be deployed over SQL Server and Oracle. Both cases are logical sets of database objects (for example, tables, indexes, and so on) owned by the same logical owner.
- **Expected Database User Schema.** OpenText Application Quality Management Database User Schema configurations, as defined in the

configuration file for a new Database User Schema. As a preparation for the current version, each project database user schema should be aligned with the latest configurations, as defined in this schema.

If you need to modify the database user schema, see the additional instructions under "Change the database user schema" on page 216.

Quick Warning Reference

This topic lists schema and data issues found in warnings generated by the verification process.

General Issues

The following table lists general issues found in verification process warnings. Some issues are fixed automatically by the repair process. Other issues require that you repair them manually.

Type	Problem	Resolution	Details
Database	Database server version not supported	manual repair	"General validation" on page 195
Database	Schema name contains invalid characters	manual repair	"General validation" on page 195
Database	Table owner does not match the server connection method	manual repair	"General validation" on page 195
Database	Repository over database feature no longer supported	manual repair	Repository over Database Feature

Type	Problem	Resolution	Details
Version control	Certain version control projects cannot be upgraded directly	manual repair	Version Control Validation
Database	Permissions	manual repair	"General validation" on page 195
Database	Configure text search	manual repair	"General validation" on page 195

Schema Issues

The following table lists schema issues found in verification process warnings. Some schema issues are fixed automatically by the repair process. Other schema issues require that you repair them manually.

Type	Problem	Resolution	Details
Table	Extra table	manual repair	"Extra Table" on page 201
Table	Missing table	repair process	"Missing Table" on page 202
Views	Extra view	manual repair	"Data validation" on page 211
Column	Extra column	manual repair	"Extra Column" on page 202
Column	Missing column	repair process	"Missing Column" on page 206
Column	Size mismatch - column size bigger than expected	manual repair	"Column Size Mismatch" on page 203

Type	Problem	Resolution	Details
Column	Size mismatch - column size smaller than expected	repair process	"Column Size Mismatch" on page 203
Column	Type mismatch	manual repair	"Column Type Mismatch" on page 204
Column	Precision	repair process	"Column Precision Mismatch" on page 204
Column	Nullable - column can accept NULL values	repair process	"Column Nullability Mismatch" on page 205
Index	Uniqueness	repair process	"Index Uniqueness Mismatch" on page 207
Index	Clustered	repair process	"Index Clustered" on page 208
Index	Missing	repair process	"Missing Index" on page 208
Constraint	Missing	repair process	"Missing Constraint" on page 208
Constraint	Extra	manual repair	"Missing Constraint" on page 208
Index	Changed	repair process	"Index Changed" on page 208
Triggers	Extra	manual repair	"Extra Trigger" on page 209
Sequence	Missing	repair process	"Missing Sequence" on page 211

Type	Problem	Resolution	Details
Sequence	Extra	manual repair	"Extra Sequence" on page 210
Sequence	Incorrect	repair process	"Incorrect Sequences" on page 211

Data Issues

The following table lists data issues found in the verification process warnings. Some data issues are fixed automatically by the repair process. Other data issues require that you repair them manually.

Type	Problem	Element	Resolution	Details
Duplicate data	Duplicate values	None	repair process	"Data validation" on page 211
Duplicate data	Duplicate IDs	None	repair process	"Data validation" on page 211
Trees	Wrong number of children	`Tables REQ/ALL_ LISTS/CYCL_ FOLD`	repair process	"Data validation" on page 211
Trees	Corrupted path	`Tables REQ/ALL_ LISTS/CYCL_ FOLD`	repair process	"Data validation" on page 211
Trees	Orphan records	`Tables REQ/ALL_ LISTS/CYCL_ FOLD`	repair process	"Data validation" on page 211
Sequences	Sequence mismatch	`Table SEQUENCES`	repair process	"Sequences" on page 210

Type	Problem	Element	Resolution	Details
Orphans	Missing parent entities	None	repair process	"Data validation" on page 211
Missing data	Missing entities	None	repair process	"Data validation" on page 211
Lists	Missing lists and values	`Tables SYSTEM_FIELD / LISTS`	repair process	"Data validation" on page 211

General validation

This topic describes the general validation checks the verification process performs.

Supported database version

The verification process checks that the project schema is stored in a supported database server. If the verification process detects that the database server version is not supported, it displays a warning.

> **Note:** For the most up-to-date supported environments, see Support Matrix

Valid Database User Schema Name

The upgrade mechanism does not support databases that include special characters in the database name. If the verification process finds special characters, you must remove them. For SQL databases, periods are also not supported in the database user schema name.

To remove special characters from database names:

1. Deactivate the project.
2. Ask your database administrator to rename the database user schema to a name that does not include special characters, or periods for SQL databases.
3. Remove the project from Site Administration.
4. Update the **Dbid.xml** file to point to the new database user schema name.
5. Restore the project by using the updated **Dbid.xml** file.
6. Run the verification process again to make sure the problem is resolved.

Mixed Table Ownership

OpenText Application Quality Management can connect to Microsoft SQL server by using SQL authentication or Windows authentication.

For each of these methods, a different user owns the tables of a project:

- **SQL Authentication.** Table owner is the user `td`.
- **Windows Authentication.** Table owner is the user `dbo` (a user mapped to the operating system user that runs the OpenText Application Quality Management server).

If you create a project with one type of authentication (for example, SQL), and then restore it with the other type of authentication (for example, Windows), these tables cannot be accessed. In this case, new tables are created with owners that are different from those of the old tables. You will not be able to work with the project. It is likely that the upgrade will fail.

To prevent this problem, the duplicate ownership validator checks that the owner of all of the tables in the project database user schema matches the connection method that OpenText Application Quality Management is using to connect to the server.

To fix table ownership manually, do one of the following:

- **SQL Authentication:** Run the following query to make `td` the table owner:

```
EXEC sp_changeobjectowner '<table name>', 'td'
```

- **Windows Authentication:** Run the following query to make `dbo` the table owner:

```
EXEC sp_changeobjectowner 'td.<table name>', 'dbo'
```

Database permissions

To enable an upgrade to the current OpenText Application Quality Management version, the project schema requires a set of minimum required permissions. The verification process makes sure that both the project user and the administrator user have all the privileges needed to perform the upgrade.

Text Search Configuration

If your database does support text search, OpenText Application Quality Management installs the required components when creating a new project database. OpenText Application Quality Management also activates the text search for the new database. The verification process checks whether your project has the text search feature enabled, and that it is configured correctly.

The verification process validates the following:

- "Validity of the Text Search Configuration" on the next page
- "Only Valid Fields Configured Under "Text Search"" on the next page
- "Text Search Validation for Oracle Database Server" on page 199
- "Text Search Validation for Microsoft SQL Database Server " on page 199

Validity of the Text Search Configuration

The verification process checks that text search components are installed and are valid on the database server. If a database server is text search-enabled in the DB Servers tab in Site Administration, text search must also be enabled on the Oracle or SQL database server. If the verification process detects that text search is not enabled or configured incorrectly on the Oracle or SQL database server, the upgrade process does not run until you manually repair the problem.

We recommend that you ask your database administrator to reconfigure text search on the Oracle or SQL database server. Alternatively, as a workaround, you can disable text search for the database server from Site Administration.

To disable the text search for the database server:

1. Run the following query on your Site Administration schema:

   ```
   update <SA Schema>.dbservers set db_text_search_enabled = null
   where dbserver_name = '<DB logical name>'
   ```

2. Restart the OpenText Application Quality Management server.
3. Run the repair process for your projects.
4. When the repair process completes, run the following query:

   ```
   update <SA Schema>.dbservers set db_text_search_enabled = 'Y'
   where dbserver_name = '<DB logical name>'
   ```

5. Restart the OpenText Application Quality Management server.

Only Valid Fields Configured Under "Text Search"

The verification process checks that only valid fields are defined as searchable. You can enable the text search only for specific entities, and only on fields of the type string or memo. The following entities are supported: BUG, COMPONENT, COMPONENT_STEP, DESSTEPS, REQ, TEST, BPTEST_TO_COMPONENT, and CYCLE. Any other configuration could cause

functionality problems during upgrade or customization. This problem is fixed automatically by the repair process.

Text Search Validation for Oracle Database Server

For an Oracle Database server, the verification process checks the following:

- **Validity of Text Search Indexes.** The verification process checks that database text search indexes are valid. Invalid text search indexes can cause functionality problems and even upgrade failure in OpenText Application Quality Management. If the verification process detects an invalid index, try to recreate the index by dropping it from the schema and creating it again. In Site Administration, click the **Site Projects** tab. Select the relevant project and click the **Enable/Rebuild Text Search** button. If this procedure returns an error, consult your database administrator or contact OpenText Support.
- **Validity of Project Database User Permissions.** The verification process checks that the project database user has the required permissions to work with text search. When text search is installed on the database, the role CTXAPP is created automatically. OpenText Application Quality Management requires that this role be granted to all projects database users that support text search. (OpenText Application Quality Management grants the CTXAPP role automatically when creating the project or enabling the text search for a project.) If this role is not granted to the project database user (configured to support text search), the verification process returns a warning. In these cases, ask your database administrator to grant the required role to the project database user.

Text Search Validation for Microsoft SQL Database Server

The verification process checks that the project database user schema enables the text search feature. To work with text search on SQL project, you need to enable the text search on the database.

To enable text search on the database:

1. Select the database from the SQL server Enterprise Manager.
2. Right-click the database name.
3. Select **Properties/Files**.
4. Select **Use Full-Text Indexing**.

Schema Validation

The verification process helps to ensure that the project database user schema is correct and configured as expected.

The verification process performs two types of schema verifications:

- **Schema Correctness.** Checks that the project database schema includes all of the required schema objects, as defined in the expected database user schema for the project. This verification ensures that all of the required entities exist and are defined as expected. It also ensures that there are no extra entities defined on top of the schema.
- **Alignment to the current version.** Notifies you about differences in the project database user schema caused by internal changes made in Quality Center or OpenText Application Quality Management. In this way, the verification process aligns the schema with the latest internal changes to the schema made in preparation for the upgrade.

The verification process displays warnings in the verification report if it finds the following:

- Extra entities defined. For example, Table, Column, Trigger, View, and Sequence.
- Differences from the expected definitions. For example, Column Size and Index Attributes.
- Missing objects.

Schema differences found by the verification process can cause upgrade failures or usage problems. As long as the verification process still finds these differences, an upgrade to the current OpenText Application Quality Management version will not start.

> **Note:** Many of the schema changes can be fixed automatically by the repair process.

The following sections contain possible warnings, grouped by the different database objects, that the verification process can display in the verification report:

Tables

This topic describes the warnings that database tables can contain.

Extra Table

The OpenText Application Quality Management schema should contain only the tables that are defined in the schema configuration file. Adding extra tables on top of the schema is not supported and might cause future problems with OpenText Application Quality Management.

Problem: If the verification process finds extra tables that were added manually to the schema, it generates an **Extra Table** warning.

> **Note:** This problem requires manual repair. The repair process cannot fix it.

Solution: Do one of the following:

- **Change the Schema.** If you use the table, copy it to a different schema. If you do not use the table, delete it. Before taking either action, back up the schema and consult your database administrator. For details, see "Change the database user schema" on page 216.

- **Use the Exception File.**

  If the project database is case sensitive, the table name must be the same in both the database and the exception file.

> **Note:** Not recommended: Instruct the upgrade to ignore this problem.

Missing Table

The verification process checks that all of the tables defined for the project schema actually exist (according to the tables of each Quality Center/OpenText Application Quality Management version).

Problem: If a table is missing, the verification process generates a **Missing Table** warning.

Solution: Do one of the following:

- See "Change the database user schema" on page 216.
- Run the repair process to create the missing table. Although you can use the repair process to add these objects, we recommend that you contact OpenText Support to make sure that the missing objects are not just symptoms of a bigger problem.

Columns

This topic covers the warnings that database columns can contain.

Extra Column

The verification process checks that each table includes the required columns, as defined for the expected database user schema and version. The schema should not include extra columns. Extra columns in a table might cause upgrade failure or functionality problems.

Problem: If the verification process detects an extra column (that does not exist in the database user schema definitions) in one of the tables, it generates an **Extra Column** warning.

> **Note:** This problem requires manual repair. The repair process cannot fix it.

Solution: Do one of the following:

- **Change the Schema.** If you have an internal implementation that requires extra table columns, move the extra columns to a different table in a different schema. If you do not use a particular column, delete it. Before taking either action, back up your schema and consult your database administrator. For a more detailed explanation, see "Change the database user schema" on page 216.
- **Use the Exception File.**

> **Note:** Not recommended: Instruct the upgrade to ignore this problem.

Column Size Mismatch

The verification process checks that all the table columns are defined as expected. This validation ensures that the column size matches the expected size as defined for each table column. This verification excludes user-defined fields, whose size can be customized through project customization.

Problem A: Size is bigger than expected. If the column size is bigger than expected, decrease the column size to the required size manually. Because this operation can cause data loss, it is not performed automatically by repair process.

> **Note:** This problem requires manual repair. The repair process cannot fix it.

Solution A: Consult your database administrator to resolve this issue. For risks involved in changing the database user schema, see "Change the database user schema" on page 216.

Problem B: Size is smaller than expected. If the column size is smaller than expected, the repair process fixes the problem automatically by increasing the column size to the expected size.

Solution B: Run the repair process to increase the current size to the required size.

Column Precision Mismatch

In an Oracle Database, "precision" is the term used to define the size of fields with the INTEGER type.

Problem: The verification process generates a warning if the precision defined for a certain column is smaller than expected.

Solution: Run the repair process to increase the current precision to the required precision.

Column Type Mismatch

Changing a column type causes the upgrade to fail, and can cause major functionality problems.

Problem: The verification process generates a **Column Type** warning if the column type has changed.

> **Note:** This problem requires manual repair. The repair process cannot fix it.

Solution: Consult your database administrator to resolve this issue. For risks involved in changing the database user schema, see "Change the database user schema" on page 216.

Column Nullability Mismatch

One of the attributes that is defined for a column is whether it can accept null values. A null is the absence of a value in a column of a row. Nulls indicate missing, unknown, or inapplicable data. If you have defined a NOT NULL or PRIMARY KEY integrity constraint for a particular column, you cannot insert rows into the column without adding a value.

Problem: The verification process compares the required definitions for each column in the expected database user schema to the project database user schema. If it encounters differences in the column NULL attribute definition, it generates a **Column Nullable** warning.

Solution: Run the repair process. The repair process runs a query to modify the column attributes to the expected attributes.

If the column includes NULL values, the repair process cannot update the column attribute to NOT NULL (if this is the required attribute) for the column. Ask your database administrator how to remove the NULL values from the column. After removing the NULL values, run the repair process again. For details, see "Change the database user schema" on page 216.

Identity Column

The IDENTITY property is one of the attributes defined for columns in Microsoft SQL server.

Problem: As part of the verification for the columns attributes, the verification process might find a column IDENTITY property that is not configured as expected.

> **Note:** This problem requires manual repair. The repair process cannot fix it.

Solution: Change the IDENTITY property of the column to the expected configuration (according to the output from the verification process report)

manually. Consult your database administrator to resolve this issue. For details, see "Change the database user schema" on page 216.

Missing Column

If a column is missing from a table, run the repair process or contact OpenText Support.

Problem: If the verification process finds that a column is missing from one of the tables, it generates a **Missing Column** warning.

Solution: Do one of the following:

- Run the repair process to fix the problem.
- See "Change the database user schema" on page 216.

Indexes and Constraints

This topic covers validations and warnings that database indexes and constraints can cause.

Overview

A database index is a data structure that improves the speed of operations in a table. You can create indexes using one or more columns, providing the basis for both rapid random lookups and efficient ordering of access to records. Database Constraints are constraints on the database that require relations to satisfy certain properties.

Extra Index

The OpenText Application Quality Management schema should include only those indexes defined in the required schema configurations.

Problem: If the verification process finds an index that is not defined in the required schema configuration, it generates an **Extra Index** warning.

> **Note:** This problem requires manual repair. The repair process cannot fix it.

Solution: Remove the extra indexes manually. Consult with your database administrator to resolve this issue. For details, see "Change the database user schema" on page 216.

Extra Constraint

The OpenText Application Quality Management schema should include only those constraints defined in the required schema configurations.

Problem: If the verification process finds a constraint that is not defined in the required schema configuration, it generates an **Extra Constraint** warning.

> **Note:** This problem requires manual repair. The repair process cannot fix it.

Solution: Remove the extra constraint manually. Consult with your database administrator to resolve this issue. For details, see "Change the database user schema" on page 216.

Index Uniqueness Mismatch

A unique index guarantees that the index key contains no duplicate values. As a result, every row in the table is unique. Specifying unique indexes on OpenText Application Quality Management data tables ensures data integrity of the defined columns. In addition, it provides helpful information that is used as a query optimizer.

Problem: If the index uniqueness attribute does not have the expected value, the verification process generates an **Index Uniqueness Mismatch** warning.

You cannot create a unique index, unique constraint, or PRIMARY KEY constraint if duplicate key values exist in the data. The verification process performs these data validations. If a table has duplicate values or IDs, based

on the index definitions on that table, the verification process also displays the duplication in the verification report. In this case, the repair process automatically fixes the duplication problem before creating the unique index.

Solution: Run the repair process to fix the problem.

Index Clustered

In Microsoft SQL, index type can be classified as clustered or non-clustered. The verification process compares the required definitions for each index in the expected database user schema to the project database user schema.

Problem: If the verification process finds differences in the index clustered attribute definition, it generates an **Index Clustered** warning.

Solution: Run the repair process to fix the problem.

Missing Constraint

Constraints are rules that the database enforces to improve data integrity.

Problem: If the verification process finds a constraint that should be defined as missing, it generates a **Missing Constraint** warning.

Solution: Run the repair process to fix the problem.

Missing Index

The verification process checks that all the required indexes (as defined in the expected database user schema) exist in the projects database user schema.

Problem: If the verification process does not find all the required indexes in the projects database user schema, it generates a **Missing Index** warning.

Solution: Run the repair process to fix the problem.

Index Changed

The verification process checks that the indexes are defined according to the expected database user schema.

Problem: If the verification process finds an index that is not defined according to the expected database user schema, it generates an **Index Changed** warning.

This warning can indicate the following problems:

- Function in a function-based index is different than expected.
- Index is not defined on the expected columns.

Solution: Run the repair process to fix the problem. The repair process removes the index, and then recreates it, based on the required definitions for this index.

Index Order Changed

The verification process checks that the order of the columns in the index definition has not changed.

Problem: If the order of the columns in the index definition has changed, the verification process generates an **Index Order Changed** warning.

Solution: Run the repair process to fix the problem. The repair process removes the index, and then recreates it, based on the required definitions for this index.

Triggers

A database trigger is procedural code that is automatically executed in response to certain events on a particular table in a database.

Database triggers can contain a warning about an extra trigger.

Extra Trigger

Extra triggers can cause upgrade failures and functionality problems.

Problem: If the verification process finds an extra trigger, it generates an **Extra Trigger** warning.

> **Note:** This problem requires manual repair. The repair process cannot fix it.

Solution: Before upgrading, back up your database schema and remove the extra triggers manually.

Because extra triggers can cause upgrade failures, the upgrade process cannot ignore this warning by using the Exception file. For details, see "Change the database user schema" on page 216.

Sequences

A sequence is an Oracle object that acts as a generator that provides a sequential series of numbers. This topic describes the warnings that database sequences can contain.

Extra Sequence

OpenText Application Quality Management schemas should contain only the sequences that are defined in the schema configuration file.

Problem: If the verification process finds an extra sequence, it generates an **Extra Sequence** warning.

> **Note:** This problem requires manual repair. The repair process cannot fix it.

Solution: Do one of the following:

- **Change the Schema.** Move the sequence to a new database user schema. Before doing so, consult with your database administrator. For details, see "Change the database user schema" on page 216.
- **Use the Exception File.**

> **Note:** Not recommended: Instruct the upgrade to ignore this problem.

Missing Sequence

Problem: If the verification process finds that one of the sequences that should be defined on the OpenText Application Quality Management schema is missing, it generates a **Missing Sequence** warning.

Solution: Do the following:

- Run the repair process to fix the problem.
- See "Change the database user schema" on page 216.

Incorrect Sequences

Problem: Sometimes the Oracle object sequence numbers become incorrect, for example, if an export of the database is done on a live activated project, in which users are still modifying tables. If the verification process finds that Oracle sequences objects are not fully synchronized with OpenText Application Quality Management schema table IDs, the verification process generates an **Incorrect Oracle sequences found** warning.

Solution: Run the repair process to fix the problem.

Data validation

One of the main functions of the verification process is to ensure that the project database contains valid data. The verification process helps you find and fix problems.

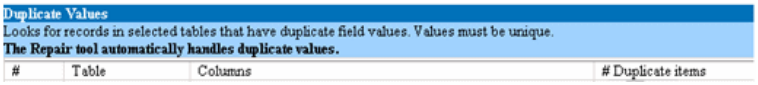
Duplicate values

Some fields (or a combination of fields) must be unique in given tables. This constraint is enforced by the creation of a unique index on these fields. For example, the combination of fields TS_SUBJECT and TS_NAME, which represent the ID of the test's parent folder and test name, must be unique. It is

not possible to create two tests with the same name under the same folder. In rare cases, a corrupted database contains duplicate values in these fields.

Problem: The verification process checks that all unique indexes exist (and therefore enforce unique values). If the verification process finds duplicate values, it does not permit the upgrade to run on the project.

The verification report specifies the fields in which there are duplications and number of duplicate values found, as shown below.


Duplicate Values
Looks for records in selected tables that have duplicate field values. Values must be unique.
The Repair tool automatically handles duplicate values.

#	Table	Columns	# Duplicate items

Solution: Automatic Repair. Run the repair process to automatically handle the duplicate values. The repair process renames the duplicate values to resolve the problem.

Duplicate IDs

Most tables have a unique primary key, usually a unique single column. If there are duplicate values in this field, the primary key is not created.

For example, in a table called test, the column TS_TEST_ID represents the test ID, which is unique. In rare cases, a corrupted database contains duplicate IDs.

Problem: The verification process checks that all IDs in a table are unique. If it finds duplicate IDs, it does not permit the upgrade to run on the project.

The verification report specifies the fields in which there are duplicate items and values, as shown below.

Duplicate IDs
Looks for records in selected tables that have duplicate ID field values.
The Repair tool automatically deletes the duplicate records.

#	Table	Column	# Duplicate Items
1	TEST	TS_TEST_ID	2

Solution: Automatic Repair. The repair process automatically deletes one of the records with a duplicate ID.

> **Caution:** This option assumes that the entire record is duplicated, and that the duplicated record is not accessible from the OpenText Application Quality Management user interface. Because there can be exceptions, we recommend that you use this option only after verifying manually that this record deletion will not cause data loss.

Tree inconsistencies

The verification process checks four different entity trees (hierarchical representation of entities):

- Test Plan tree
- Business Components tree
- Requirement tree
- Test Lab tree

The verification process checks that the data in the tree tables is correct.

> **Caution:** Do not manually fix any problems related to tree data. The repair process fixes them automatically.

Problem: The verification process checks for the following types of problems:

- **Corrupted Path.** This is an internal OpenText Application Quality Management field that contains a string that represents the order of each node in the tree.
- **Wrong Number of Children.** This is an internal OpenText Application Quality Management field that contains the number of children for each node in the tree.
- **Orphan Records in Trees.** By definition, orphan records do not have parent records. As a result, you cannot access them through the OpenText Application Quality Management user interface.

Solution: Automatic Repair. Run the repair process to automatically fix any problems related to tree data.

> **Caution:** Before beginning the automatic repair, review each orphan record carefully. If the verification process finds an orphan record, it deletes it (and all its descendants) from the tree automatically.

Views

Database views can contain a warning about extra views.

OpenText Application Quality Management schemas should contain only the views that are defined in the schema configuration file.

Problem: If the verification process detects extra views that were added manually to the schema, it displays an **Extra Views** warning. Adding extra views on top of the schema is not supported and could cause problems.

> **Note:** This problem requires manual repair. The repair process cannot fix it.

Solution: Do one of the following:

- **Change the Schema.** If you use the view, copy it to a different schema. If you do not use the view, delete it. Before taking either action, back up your schema and consult your database administrator. For details, see "Change the database user schema" on page 216.
- **Use the Exception File.**

> **Note:** Not recommended: Instruct the upgrade to ignore this problem.

Orphaned entities

The verification process checks for entity data that is missing corresponding parent data. For example, the following entities might be missing corresponding test configurations or test criteria:

- Test configuration coverage
- Criteria coverage
- Run criteria
- Runs
- Test instances

> **Caution:** Do not manually fix any problems related to orphaned entities. The repair process fixes them automatically.

Problem: In version-controlled projects, deleting a test configuration or test criteria did not delete corresponding entities after checking in. This caused incorrect coverage calculation.

Solution: Automatic Repair. Run the repair process to automatically fix any problems related to orphaned entities created by this problem.

Missing entities

The verification process checks for data that is missing. For example, the following entities might be missing:

- Test configurations
- Test criteria

> **Caution:** Do not manually fix any problems related to missing entities. The repair process fixes them automatically.

Problem: The upgrade process can detect that certain entities are missing based on information that exists in related tables.

Solution: Automatic Repair. Run the repair process to automatically fix any problems related to missing entities created by this problem.

Missing lists and/or list values

The verification process checks that all of the fields of List type are associated with a list.

Problem: If a list and/or its values are missing, the verification process generates a warning about missing lists or missing list values.

Solution:

Run the repair process to create the missing list and/or its values.

Missing lists are re-created with the name: **AUTO_GENERATED_LIST_NAME_*<unique_number>***

After running the repair process, do the following in **Customization > Project Lists**:

- Rename any lists whose names are prefixed by **AUTO_GENERATED_LIST_NAME_**.
- If necessary, add any list values that are missing.

> **Tip:** Although you can use the repair process to add these objects, we recommend that you contact OpenText Support to make sure that the missing objects are not just symptoms of a bigger problem.

Change the database user schema

This topic describes the problems that require manual repair (cannot be fixed automatically by the repair process), and recommends solutions for these

problems. If you encounter any of the problems mentioned below, consult with your database administrator or contact OpenText Support for further guidelines to resolve these problems before upgrading.

The stability of the new database upgrade component depends on the database user schema validity. We recommend that you not use the Exception file to change the database user schema.

Missing database objects

Missing database objects can be symptoms of a bigger problem.

Problem: Missing database objects (for example, tables and indexes) can yield unexpected and unwanted behavior.

Solution: Although you can use the repair process to add these objects, we recommend that you contact OpenText Support to make sure that the missing objects are not just symptoms of a bigger problem.

Missing list warning

User-defined fields of List type must be associated with lists.

Problem: If a list is missing for a user-defined field, the verification process generates a **Missing List** warning.

Solution: Contact OpenText Support for instructions on changing the data type of the user-defined field from List to String in the SYSTEM_FIELD table.

Caution: Contact OpenText Support before attempting to fix the problem manually.

Sequences warning

An internal mechanism manages IDs and other system numerators. The table SEQUENCES holds the name of the table or other entity whose numeration is being tracked as well as its highest current value.

Problem: If one of the records is missing in this table, or if one of the values is incorrect, the verification process generates a **Sequences** warning.

Solution: The repair process fixes the problem automatically.

> **Caution:** We strongly recommend that you not attempt to fix the problem manually.

Changed database objects

Any of the following cases is defined as a Changed Database Object:

- Data type of a column was changed
- Length of a column was changed
- Nullability of a column was changed
- Column is defined as identity although it should not be defined as such, or vice versa

Problem: A changed column data type can result in incorrect behavior on the server side.

Solution: To avoid this behavior, make sure that you have resolved all data type and length concerns before beginning the upgrade.

For every changed database object that is found, do the following:

1. Create a new column with the required attributes as originally defined by the OpenText Application Quality Management server.

2. Move the data from the old column to the new one.

   If you cannot move the data (for example, move strings to numeric columns, or move large data to smaller fields), contact OpenText Support.
3. Remove the old column.
4. Rename the new column to the original column name.

Extra database objects

OpenText Application Quality Management has various customization options. One option is to add user-defined fields (UDFs). You can add a UDF by using either the project customization user interface or through OTA (Open Test Architecture).

Problem: Any other addition to the database user schema (for example, defining extra objects on top of OpenText Application Quality Management schema) can result in a failure, such as the following:

- **Name Conflict.** If the later version happens to include a name that you added for a proprietary database object (for example, a table, view, or column), the two names will be in conflict.
- **Copy and Synchronize Failure.** If the database user schema contains extra or missing database objects, some OpenText Application Quality Management mechanisms for copying and synchronizing might fail.
- **Extra Triggers.** If the database contains extra triggers, some update operations might fail.

Solution:

For each extra database object that is found, perform the corresponding solution:

- **Move extra columns to newly created tables.**

To make sure a new table has a one-to-one relationship with the original table, define the primary key of the new column in the new table with the value of the primary key of the original column in the original table.

- **Move extra tables to a different database user schema.**

  These extra tables include those tables created above. You might need to amend the proprietary application data access of these tables. You can still access these tables from within the OpenText Application Quality Management database connection by specifying the full name.

  - Oracle

    ```
    <schema name>.<table name>
    ```

  - SQL Server

    ```
    <database name>.td.<table name>
    ```

  To be able to see these tables, you must grant the necessary permissions for the database user schema.

- **Move extra views to a different database user schema.**

  Like extra tables, these views can be moved to a different database user schema. In addition, you must grant reading permissions to the newly created database user schema on the database user schema objects.

- **Remove referential integrity between customer database objects and OpenText Application Quality Management database objects.**

  This removal includes no data loss.

- **Remove extra triggers before the upgrade, and, only if truly necessary, restore them after the upgrade.**

  No data loss is involved. The upgrade process includes data upgraders that perform some data manipulations (for example, removing duplicate values, fixing tree structures, and so on).

  Your triggers will not be invoked on these update events.

As a result, you need to do the following:

a. Ask OpenText Support for information about the data upgrader activity.
b. Review the information about the data upgrader activity.
c. Decide on which proprietary updates you need to perform.

- **Remove extra indexes.**

  You can log all indexes before the upgrade, and (only if necessary) restore them after the upgrade. No data loss is involved.

- **Oracle Database only: Move extra sequences to a newly created database user schema.**

  To access the extra sequences from the database user schema, you must grant OpenText Application Quality Management the required permissions. When moving these sequences, set them to start with the number they reached at the time of the move.

Troubleshooting the installation

This section contains troubleshooting suggestions for issues relating to the installation.

This section includes:

Disabling validation checks for the installation wizard

The Installation Wizard automatically performs validation checks to verify that particular system configurations requirements are met. If the configuration does not complete due to a failed validation, you can fix the problem or disable selected validation checks, and rerun the installation.

> **Note:**
>
> - You should disable validation checks only if you decide to take responsibility for the ALM server installation.
> - To resolve failures that occur during the Installation Wizard, see "Checking the installation and configuration log files" on page 227.
> - For troubleshooting tips on database validations, see "Database validator fails" on page 229.

To disable configuration validators and rerun the Installation Wizard in Linux or Windows silent installation:

1. In the installation directory, locate the **validations.xml** file, which is near the installation executable (**ALM_installer.bin**).
2. Edit the **validations.xml** file by changing the validation value from **true** to **false** as required. Following is an example of the file with all configuration validators active.

```
<validations>
        <os enabled="true" />
        <memory enabled="true" threshold="8" />
        <installation_disk_space enabled="true"
threshold="8" />
        <sa-schema enabled="true" />
        <db enabled="true" />
        <mail enabled="true" />
        <license-key enabled="true" />
        <repository enabled="true" />
        <sa-user enabled="true" />
        <security enabled="true" />
        <alm-services enabled="true" />
        <web-server enabled="true" />
</validations>
```

3. Save the file and rerun the installation.

Configuration Validators

Validator	Checks	To Disable
os	Checks that the operating system is supported. **Note:** For the most up-to-date supported environments, see http://admhelp.microfocus.com/alm/specs/alm-qc-system-requirements.htm.	<os enabled="false" />
memory	Checks that the customer machine has at least x GB of memory (x is defined by the threshold value, the default is 8 GB).	<memory enabled="false" />

Validator	Checks	To Disable
installation_disk_space	Checks that the installation location has at least x GB of free disk space (x is defined by the threshold value, the default is 8 GB). **Note:** This validation is related only to the installation location. If the installation fails because of a lack of free space in the temporary folder, changing the threshold value or disabling this validation does not affect the failure.	<installation_disk_space enabled="false" />
sa-schema	Checks Site Administration database settings.	<sa-schema enabled="false" />
db	Checks database connectivity.	<db enabled="false" />
mail	Checks that the mail server is valid.	<mail enabled="false" />
license-key	Checks the license file key.	<license-key enabled="false" />
repository	Checks that the repository folder is accessible, and has sufficient space.	<repository enabled="false" />
sa-user	Checks site administrator user settings.	<sa-user enabled="false" />
security	Checks encryption passphrases.	<security enabled="false" />

Validator	Checks	To Disable
alm-services	Checks Windows service settings.	<alm-services enabled="false" />
web-server	Checks that the HTTP port and web server deployment folder is accessible, and has sufficient space	<web-server enabled="false" />

To disable configuration validators and rerun the Installation Wizard in Windows:

> **Note:** These instructions do not apply when running the Windows silent installation. For Windows silent installation, follow the instructions above.

1. In the installation directory, locate the **validations.xml** file, which is near the installation executable (**ALM_installer.exe**).
2. Edit the **validations.xml** file by changing the validation value from **true** to **false** as required. Following is an example of the file with all configuration validators active.

```
<validations>
        <os enabled="true" />
        <memory enabled="true" threshold="8" />
        <installation_disk_space enabled="true"
threshold="8" />
        <sa-schema enabled="true" />
        <db enabled="true" />
        <mail enabled="true" />
        <license-key enabled="true" />
        <repository enabled="true" />
        <sa-user enabled="true" />
        <security enabled="true" />
        <alm-services enabled="true" />
        <web-server enabled="true" />
</validations>
```

3. Only the following configuration validators are used in the Windows installation wizard:

Validator	Checks	To Disable
os	Checks that the operating system is supported. **Note:** For the most up-to-date supported environments, see http://admhelp.microfocus.com/alm/specs/alm-qc-system-requirements.htm.	<os enabled="false" />
memory	Checks that the customer machine has at least x GB of memory (x is defined by the threshold value, the default is 8 GB).	<memory enabled="false" />
installation_disk_space	Checks that the installation location has at least x GB of free disk space (x is defined by the threshold value, the default is 8 GB). **Note:** This validation is related only to the installation location. If the installation fails because of a lack of free space in the temporary folder, changing the threshold value or disabling this validation does not affect the failure.	<installation_disk_space enabled="false" />
db	Checks database connectivity.	<db enabled="false" />

4. Save the file and rerun the installation.
5. On the Installation Summary page, before clicking **Done**, edit the **run_configuration.bat** file, located under <installation folder>\ALM, to disable validations.

Validator	Checks	To Disable
Existing installation	Checks if an older version of ALM or Quality Center is installed.	- wPreviousInstallationValidator
License file	Checks license file key.	-wLicenseTypeValidator
Security passphrases	Checks encryption passphrases.	-wEncryptionStepValidator
Mail server	Checks that the mail server name is valid.	wMailServerValidator
Database settings	Checks Site Administration database settings.	-wSaSchemaValidator
Site administrator	Checks site administrator user settings.	-wSiteAdminUserValidator
repository folder	Checks that the repository folder is accessible, and has sufficient space.	-wRepositoryValidator

6. Save the **run_configuration.bat** file and click **Done** to continue the installation.

Checking the installation and configuration log files

If you encounter problems installing ALM, check for errors in the log files.

Windows

Windows File Delivery Logs

Log	Path
Install Completed	<Deployment folder>\ALM\log
Install Failed	on the desktop: Application_Lifecycle_Management_Install_<mm_dd_yyyy_hh_mm_ss>.log

Application logs

Log	Path
Configuration logs	<installdir>\log
Site Administration database schema creation logs	<installdir>\log\sa

Linux

Delivery logs

Log	Path
Install Completed	<Deployment folder>/ALM/log
Install Failed	in the user's home folder: Application_Lifecycle_Management_Install_<mm_dd_yyyy_hh_mm_ss>.log

Application logs

Log	Path
Configuration logs	<installdir>/log
Site Administration database schema creation logs	<installdir>/log/sa

Installation already exists

After uninstalling a previous version, an error message displays while installing a later version, indicating that OpenText Application Quality Management already exists.

Perform the following steps:

1. Navigate to the **C:/ProgramData** directory.
2. Locate the the InstallAnywhere global registry file (hidden file), search for **.com.zerog.registry.xml**. Edit the file and remove the sections related to OpenText Application Quality Management and its components.
3. Locate the **.com.zerog.registry.xml.swp** (hidden file). If the file exists, delete it.

Database validator fails

During the server configuration, the database validator performs the following checks:

- Check that the input parameters are correct.
- Check that the Site Administration database schema name was provided.
- Check whether the same authentication type was used as the one used in the previous installation.

Perform the following steps:

1. Check whether the parameters are correct:
   - Read the error message that displays during installation and try to understand and resolve the problem from the root cause.
   - For further clarifications, check with your database administrator.
   - If no error was found and you are sure that the parameters are correct,

disable the DB parameters validator. For details, see "Disabling validation checks for the installation wizard" on page 222.

2. Check that the Site Administration Database Schema name was provided:
   a. Open a database query tool.
   b. Make sure the **PROJECTS** table exists in the Site Administration Database Schema. This table does not exist in the project schema.
3. To check the authentication type of a previous installation:
   a. Navigate to **<Installation path>\ALM\application\20qcbin.war\WEB-INF** and open the siteadmin.xml file in a text editor.
   b. Search for the **native** property. If its value is set to **Y**, Windows authentication was used. Make sure that the new installation uses the same authentication type (Microsoft SQL Server authentication or Windows authentication) as the previous installation.

Monitoring server fails

When running one of the Java-based tools to monitor OpenText Application Quality Management you receive the following message:

"Not enough storage is available to process this command."

This problem is caused because the JVM running the server is running with a service account.

Choose one of the following solutions, depending on which tool you are running:

- **jmap and jstack.**

  See the suggestion from Stack Overflow about "Jstack and Not enough storage is available to process this command".

  You will be required to download the PsExec tool from Microsoft.

- **jconsole and jvisualvm.**

  Refer to the Microsoft article about creating a user-defined service.