opentext™

OpenText™ Documentum™ Content Management

On-Premises Upgrade and Migration Guide

Upgrade and migrate the on-premises applications.

EDCCS250400-UMD-EN-01

OpenText™ Documentum™ Content Management
On-Premises Upgrade and Migration Guide
EDCCS250400-UMD-EN-01
Rev.: 2025-Oct-21

This documentation has been created for OpenText™ Documentum™ Content Management CE 25.4.
It is also valid for subsequent software releases unless OpenText has made newer documentation available with the product, on an OpenText website, or by any other means.

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Tel: +1-519-888-7111
Toll Free Canada/USA: 1-800-499-6544 International: +800-4996-5440
Fax: +1-519-888-0677
Support: https://support.opentext.com
For more information, visit https://www.opentext.com

Table of Contents

Chapter 1

Overview

This guide is for IT personnel who are upgrading the OpenText Documentum Content Management (CM) system, including OpenText Documentum CM custom applications.

This guide describes how to upgrade a OpenText Documentum CM system and migrate customizations to the upgraded OpenText™ Documentum™ Content Management Server. Refer to the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* for additional detailed planning information.

- All references to *6.7 SP2 and later* in this document refer to OpenText Documentum CM 6.7 SP2 and all versions that follow it, including OpenText Documentum CM 7.x.
- All references to *7.x* in this document refer to OpenText Documentum CM 7.0, 7.1, 7.2, and 7.3.
- All references to *16.x* in this document refer to OpenText Documentum CM 16.4, 16.7, and 16.7.1.
- All references to *20.x* in this document refer to OpenText Documentum CM 20.2, 20.3, and 20.4.
- All references to *21.x* in this document refer to OpenText Documentum CM 21.1, 21.2, 21.3, and 21.4.
- All references to *22.x* in this document refer to OpenText Documentum CM 22.1, 22.2, and 22.4.
- All references to *23.x* in this document refer to OpenText Documentum CM 23.2 and 23.4.
- All references to *24.x* in this document refer to OpenText Documentum CM 24.2 and 24.4.
- All references to *25.x* in this document refer to OpenText Documentum CM 25.2 and 25.4.

The following table provides a definition of the commonly used terms in this guide.

Term	Definition
Upgrade	Refers to moving seamlessly from a previous version of the software to a more recent version. When hardware and third-party applications are compatible with the new version, and the existing version supports direct upgrade, an in-place move from an earlier version of OpenText Documentum CM components can be performed.
Migration	Refers to moving customizations from one OpenText Documentum Content Management (CM) Server instance to another. It can refer to moving from an unsupported environment to a supported one, such as an upgrade that cannot be done in place due to lack of compatibility or the need to update/change hardware, or the need to move from an unsupported environment to a supported one. It can also refer to moving data from one location, server, or repository to another. The process of migration involves creating a repository and then copying the content from the old repository to the new repository.
Compatibility	Refers to software components that are intended to work together seamlessly. For example, different clients that can independently modify objects in the repository without conflicts, or an environment where Documentum CM Server applications, repositories, or client applications of different versions coexist in an implementation (mixed version environments) without conflicts or errors.

Chapter 2

Upgrade and migration overview

This chapter provides a conceptual overview of upgrade and migration of a OpenText Documentum CM instance.

2.1 Upgrade and migration

This guide covers upgrade and migration of OpenText Documentum CM applications.

You must be on OpenText Documentum CM 16.4 Patch 42 to perform an in-place upgrade to OpenText Documentum CM 25.x. The product *Release Notes* provides information about the supported operating system and database in OpenText Documentum CM 25.4.

Note: The upgrade and migration guide that is included with your source and target versions provides instructions on upgrading from a version earlier to OpenText Documentum CM 6.7 SP2.

Migration refers to moving from an unsupported version to a supported version of the same operating system and database. It does not refer to moving from one operating system/database to another. Migration between operating system or database requires a new installation and engagement with OpenText Global Technical Services.

You can migrate existing customizations such as DocApps, Documentum Archive (DAR) files, and business objects. "Upgrade and migration of components" on page 11 shows components that can be migrated, upgraded, or both.

Table 2-1: Upgrade and migration of components

Component	Migrate	Upgrade
Documentum CM Server	X	X
Custom DocApp/DAR files	X	
Service-based Business Objects (SBOs)	X	
Type-based Business Object (TBOs)	X	
Java methods	X	X

If you are installing a new Documentum CM Server instance, move and modify (as required) the custom Java methods, DocApps, DARs, SBOs, and TBOs to the new Documentum CM Server instance.

Notes

- DocApps, SBOs, TBOs (BOF2 version), and Java methods bundled as SBOs continue to work in an upgraded Documentum CM Server.
- You can disable the new features or activate prior features that have been deprecated or turned off by default for OpenText Documentum CM 25.x. This guide does not describe new features, except where they change or replace existing behavior in custom applications.

Check the installation guide for each application that you are upgrading for specific considerations.

Before you perform the upgrade, check the list of products that are compatible with OpenText Documentum CM 25.x in the product *Release Notes*.

The *OpenText Documentum Content Management - Server System Object Reference Guide (EDCCS250400-ORD)* provides information about new, changed, deprecated, and obsolete object types and properties.

For information about deprecated, new, and obsolete properties in `dfc.properties`, see `dfcfull.properties`.

2.2 Understanding migration

Migration is a straightforward process. You document the current configuration, plan your upgrade configuration, and then upgrade the individual system components in a sequence that minimizes impact on your users.

Migration can be separated into two basic tasks:

- Install and configure OpenText Documentum CM 6.7 SP2 or later software.
- Move configurations and customizations to the new servers.
  - Enable features that you want to keep.
  - Disable new features that you do not want.
  - Enable new features for existing custom components.

The "Migrating Documentum CM Server" on page 185 chapter provide more information about the migration process.

Most of the features in OpenText Documentum CM 6.7 SP2 and later versions are enabled by default. This guide provides the steps for enabling features that are not enabled by default.

2.3 Order of new product installation

Figure 2-1 shows the recommended installation order for new OpenText Documentum CM systems. The *server* in this diagram is the host for the Relational Database Management System (RDBMS), Documentum CM Server, or Index Server.

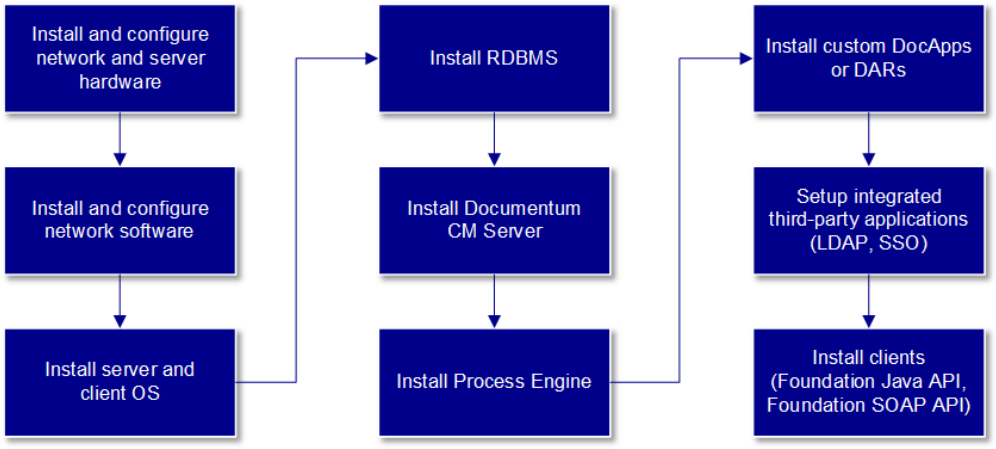


Figure 2-1: System installation order, new OpenText Documentum CM system

The recommended installation and upgrade order for new OpenText Documentum CM systems is as follows:

1. OpenText™ Documentum™ Content Management Server
2. OpenText™ Documentum™ Content Management Administrator
3. OpenText™ Documentum™ Content Management XML Store
4. OpenText™ Documentum™ Content Management Content Storage Services
5. OpenText™ Documentum™ Content Management Trusted Content Services
6. OpenText™ Documentum™ Content Management Content Services for Centera
7. OpenText™ Documentum™ Content Management Content Intelligent Services
8. OpenText™ Documentum™ xPlore
9. OpenText™ Documentum™ Content Management High-Volume Server
10. OpenText™ Documentum™ Content Management Transformation Services
11. OpenText™ Documentum™ Content Management Thumbnail Server
12. OpenText™ Documentum™ Content Management Branch Office Caching Services
13. OpenText™ Documentum™ Content Management Foundation SOAP API, including any custom OpenText Documentum Content Management (CM) Foundation SOAP API applications

14. OpenText™ Documentum™ Content Management Foundation CMIS API, including any custom OpenText Documentum Content Management (CM) Foundation CMIS API applications
15. OpenText™ Documentum™ Content Management Foundation Java API, including any custom OpenText Documentum Content Management (CM) Foundation Java API applications
16. OpenText™ Documentum™ xCelerated Composition Platform 2.x
    - OpenText™ Documentum™ Content Management Process Engine
    - OpenText™ Documentum™ Process Integrator

The coexistence of xCP 2.x and OpenText Documentum CM 6.7.x applications on the OpenText Documentum CM 7.x exists. The 6.7 SP2 version of the upgrade and migration guide provides information about the coexistence of xCP 2.x and OpenText Documentum CM 6.7.x applications scenarios.

2.4 Order of system updates

Figure 2-2 shows the recommended order in which to upgrade system components. The *server* in this diagram is the host for the RDBMS, Documentum CM Server, or Index Server.

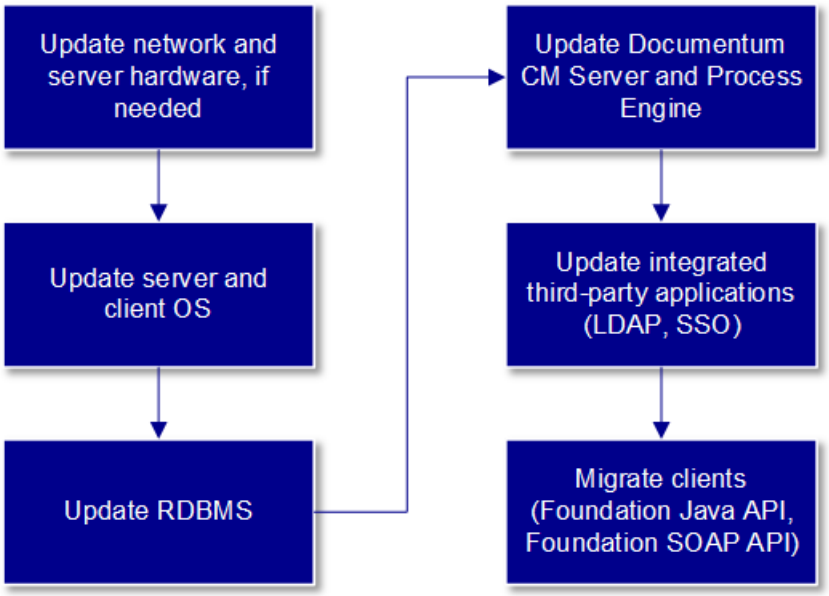


Figure 2-2: System update order, existing OpenText Documentum CM system

Caution

For Documentum CM Server, host operating system, or RDBMS upgrades, ensure that the product version is supported by the Documentum CM

Server version you are installing. For application server operating system or server upgrades, ensure that the product version is supported by the WDK-based application you are installing.

In some cases, you must uninstall upgrades to existing OpenText Documentum CM system installations before installing a new version.

The product *Release Notes* provides information on OpenText Documentum CM product compatibility. When there are version compatibility restrictions, upgrading one product generally requires upgrading interoperating products to the same version or to a major version family. In most cases, compatibility conflicts result from client applications that add new functionality to Documentum CM Server. In these cases, upgrading Documentum CM Server before the client application is especially important.

Chapter 3

Planning the OpenText Documentum CM system upgrade

Upgrading a system requires planning. Know your starting point, choose a destination, then pick the best route to get there. This chapter provides some practical advice for plotting your course from OpenText Documentum CM 6.7 SP2, 7.x, 16.x, 20.x, 21.x, 22.x, 23.x, 24.x to 25.x.

3.1 System upgrade strategies

A OpenText Documentum CM system upgrade involves development, test, and production phases.

- Development: In this phase, you move customizations from an old product version to the new version and then verify that they still work properly.
- Test: In this phase, you deploy and run the full set of products to emulate the production system as closely as possible. This is frequently done on virtual hosts. After all your system tests pass, you can upgrade the production system.
- Production: In this phase, you upgrade the existing production system in place with the verified customizations.

Note: The Documentum CM Server/database component (the repository) is the only part of the system for which there is an upgrade script. All other system product components require fresh installation.

The upgrade strategy provided in this section addresses upgrading all products in the system to the same version number, resulting in a homogeneous system.

Figure 3-1 shows the high-level decision points involved when moving from a test system to a production system. Functional testing of new customizations and manual migration of existing customizations into new client version is a part of the development phase.

If you want to upgrade the repository, create a copy of the production repository in your test system on which you can run the upgrade. "Setting up a test environment" on page 26 provides more information about creating a repository copy. If you want to change the database operating system, you can use the utilities available through the third-party database to export the database and import it into a new database instance on the different operating system. After running the Documentum CM Server configuration program to reestablish the connection between the existing Documentum CM Server instance and the new database instance, run Documentum CM Server to upgrade the entire repository.

Note: If you want to upgrade the repository configured with the certificate-based SSL mode and if you want to upgrade the AEK key, convert the primary server to the anonymous SSL mode and then perform the upgrade process as described in "Upgrading Documentum CM Server" on page 35 and/or "Upgrading scenarios" on page 75.

After the successful upgrade, to enable the certificate-based SSL mode manually, do one of the following tasks:

- If HashiCorp Vault is enabled, add the certificate password secret ID in the password files of certificates as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.
- If HashiCorp Vault is not enabled, after the upgrade process is completed, regenerate the password files of certificates.

Then, restart the repository.

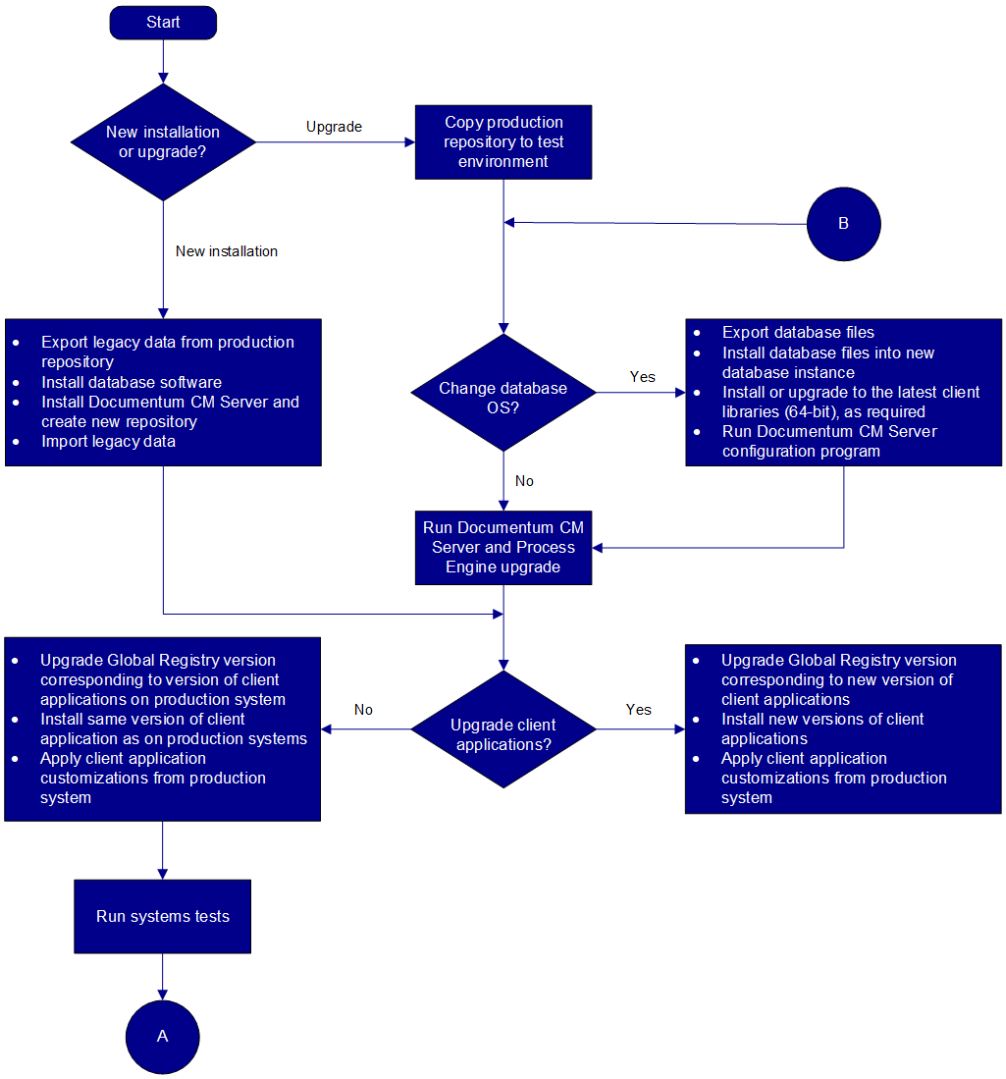
If you are performing a fresh install instead of an upgrade, migrate your data files to the new Documentum CM Server and database instances. To migrate your content to the new OpenText Documentum CM instance, choose the OpenText or third-party tool or service suited for your needs.

A OpenText Documentum CM system requires a global registry repository that matches the version family of the system clients. The global registry is a central location used to store common objects used by all repositories, such as SBO network locations, OpenText Documentum Content Management (CM) Branch Office Caching Services settings, and user settings. After installing or upgrading the test system repository, install a global registry repository that matches the version of the client applications, and install the client software. If your client software versions are to remain as the same version as your production system, you can copy the customized files from your production system directly over to the same version client instance on the test system. If the client version software is different, migrate your customizations to the new client files.

After migrating to the test system, ensure that your system is running properly by conducting system tests. After all your system tests pass, you can upgrade the production system. Typically, your production system is taken offline for a weekend while performing an in-place upgrade.

Note: You can use virtual machine hosts for the entire system or for system components. Using virtual machines, you can swap out pre-upgraded system images on the same physical host to minimize the downtime of an in-place upgrade.

The production system contains new content and full-text indexes generated since the repository was copied or you migrated your data to the new repository.


Start
New installation or upgrade?
Upgrade
Copy production repository to test environment
B
New installation
Export legacy data from production repository
Install database software
Install Documentum CM Server and create new repository
Import legacy data
Change database OS?
Yes
Export database files
Install database files into new database instance
Install or upgrade to the latest client libraries (64-bit), as required
Run Documentum CM Server configuration program
No
Run Documentum CM Server and Process Engine upgrade
Upgrade Global Registry version corresponding to version of client applications on production system
Install same version of client application as on production systems
Apply client application customizations from production system
No
Upgrade client applications?
Yes
Upgrade Global Registry version corresponding to new version of client applications
Install new versions of client applications
Apply client application customizations from production system
Run systems tests
A

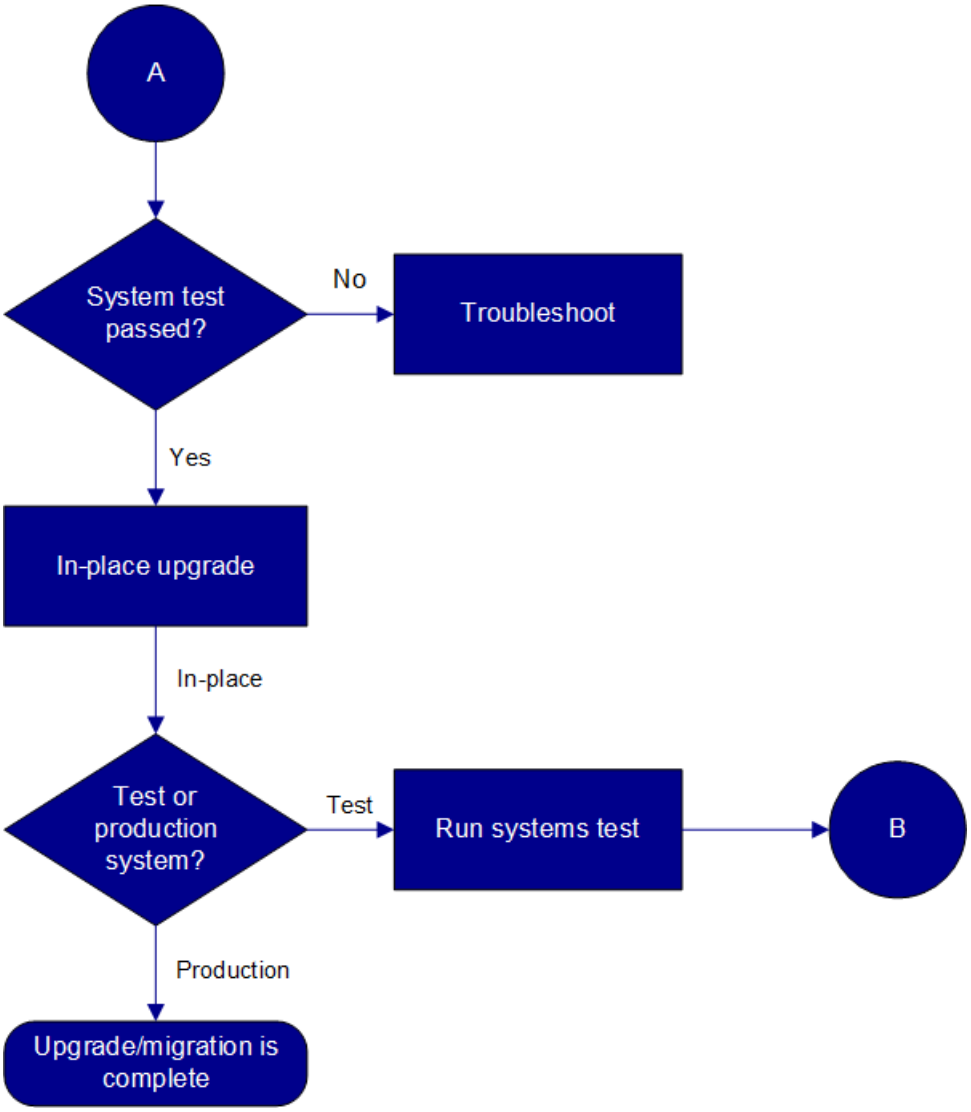


Figure 3-1: System upgrade scenarios

3.2 Changes that impact Documentum CM Server upgrade or migration

This section describes miscellaneous changes that can affect the migration to Documentum CM Server 25.x.

3.2.1 Upgrading multiple repositories to the same version

When upgrading Documentum CM Server from 6.7 SP2 or later to 25.x, first upgrade the software and then the repository.

If Documentum CM Server comprises of multiple repositories, ensure that you upgrade all repositories to 25.x. You cannot have multiple repositories of different versions on the same Windows host since different method server binaries are used for different versions.

It is recommended that you upgrade all repositories in Documentum CM Server to the same version.

3.3 Mapping your current configuration

The following system configuration diagrams and sample worksheets provide a starting point for documenting the infrastructure of your current system. You may already have similar diagrams from which you can get much of this information. If you do not, be sure to keep a copy of the existing plan to help with future migrations.

Take the time to verify that any existing diagrams reflect the current configuration.

Complete one copy of "Documentum CM Server and database server host worksheet" on page 21 for each server host and client configuration used in your current system (for example, Documentum CM Server, full-text indexing server, Federated Search Server, or application server).

Table 3-1: Documentum CM Server and database server host worksheet

Item	Value
Hardware and Processors	
Memory	
Operating system and version	
Documentum CM Server version	
RDBMS and version	
Repository size	Number of objects: Storage space required:

Item	Value
Global Registry	[ ] Yes [ ] No
Java/JRE version	
Foundation Java API version	
Other product version	
Other product version	
Other product version	

Table 3-2: Web application server host worksheet

Item	Value
Hardware and processors	
Memory	
Operating system and version	
HTTP Server version	
Java version	
Foundation Java API version	
Other product and version	
Other product and version	
Other product and version	

Table 3-3: Index server host worksheet

Item	Value
Hardware and processors	
Memory	
Operating system and version	
HTTP server version	
Java version	
Foundation Java API version	
Other product and version	
Other product and version	
Other product and version	

Table 3-4: Client machine worksheet

Item	Value
Operating system and version	
Browser and version	
Java version	
Other product and version	
Other product and version	
Other product and version	

Table 3-5: Customized components worksheet

Product	Customized Components	Customization type	Customization Description	Disposition
				• 6.7 SP2 and later Compatible • Needs changes • Obsolete
				• 6.7 SP2 and later Compatible • Needs changes • Obsolete
				• 6.7 SP2 and later Compatible • Needs changes • Obsolete

3.4 Designing a OpenText Documentum CM 25.x configuration

This section discusses some of the design decisions you must make before implementing a OpenText Documentum CM 25.x configuration. Departmental systems are configurations where Documentum CM Server, RDBMS, and global registry all reside on the same host machine. Enterprise systems are configurations containing multiple Documentum CM Servers, data repositories, and distributed services to improve performance in high traffic or geographically dispersed environments.

3.4.1 Addressing hardware concerns

Verify that the hardware you are currently using will continue to meet your needs for the foreseeable future. In particular, if you have been hosting more than one server on a single machine (for example, Documentum CM Server and an application server), this is a good time to divide the functions between two or more server hosts to boost performance. When upgrading to OpenText Documentum CM 25.x, ensure that at least 10 GB of memory is available.

You can also make an estimation on the required memory by calculating the memory consumption of each of the OpenText Documentum CM executables. The following table lists the memory consumption for each executable of OpenText Documentum CM based on their count.

Table 3-6: Memory consumption by OpenText Documentum CM executables

OpenText Documentum CM executable name	Count	Memory consumption (MB)
DMBASIC method server (Master)	1	1
Agent	5	2560 **Note:** Each agent requires 512 MB of memory.
Java Method Server	1	1300
Agent executable	1	512
Documentum.exe	1	X
Total	9	4.373 GB

Note: The table lists the memory consumption for a single repository if the database is installed in another machine. If you have multiple repositories, multiply the total memory with the number of repositories. For example, if you have two repositories, the total memory required would be 8.6 GB (that is, 2 X

4.3). The memory consumptions values are derived or obtained after testing the product in the testing environment. Every effort is made to simulate common customer usage scenarios but actual results may vary due to differences in hardware and software configurations, data, and other variables.

3.4.2 Upgrading third-party software

Verify that the third-party software, such as operating system, database, and so on, you are currently using with the existing version is still supported, or upgrade to the supported versions as necessary. If the third-party component does not have a direct upgrade path to the supported version, then there is no direct upgrade path for the Documentum CM Server upgrade. The product *Release Notes* provides information about supported third-party software version.

3.4.3 Planning for global registries

Designate one of the repositories in your version 6.5 or later system as the *global registry*. Decide which of your repositories to use as the global registry. If you already have a OpenText Documentum CM 5.3 SP6, 6.0, or 6.0 SPx global registry, upgrade to OpenText Documentum CM 25.x.

During repository configuration, you are prompted with the message **Do you want to add this repository to another global repository**. You can select one of the following options:

- **Yes**

  Provide the repository name and the login credentials (user login name and password) of the global registry user in that repository. The Foundation Java API instance on the current host is configured to access the remote global registry repository.

  – If HashiCorp Vault is enabled, the global registry password is retrieved from the HashiCorp Vault server.

  – If HashiCorp Vault is not enabled, type the global registry password.

- **No**

  Provide a user login name and password for the global registry user in the repository you are currently configuring. Record the login name and password; use this login name and password to configure other repositories in your system to allow them to access the global registry. The local Foundation Java API instance is also configured to access this global registry.

  – If HashiCorp Vault is enabled, the global registry password is retrieved from the HashiCorp Vault server.

  – If HashiCorp Vault is not enabled, type the global registry password.

Regardless of whether you designate the repository as a global registry or not, the global registry user is created for all repositories. The global registry user (dm_bof_registry), is the repository user whose account Foundation Java API clients

use to connect to the repository to access required service-based objects and user information. The user has read access to objects in /System/Modules only.

If you do not configure the repository as a global registry, the user is created with a default value for the login name, and the user state is set to `Inactive`.

If you want to enable the repository as a global registry later, use OpenText Documentum Content Management (CM) Administrator to change the user state to `Active` and provide the user with a user login name and password that you choose. Make sure that you follow the password complexity rules. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about password complexity rules and to enable the repository as a global registry.

3.4.4 Mapping a OpenText Documentum CM 25.x configuration

For each server host and client configuration, complete a planning document. You can use the same forms used for mapping your current configuration (see "Mapping your current configuration" on page 21).

3.5 Planning upgrade and migration to OpenText Documentum CM 25.x

Now that you know your starting point and your destination, you can choose the best upgrade and migration path. The recommended configuration is a homogeneous OpenText Documentum CM 6.5 or later system. The migration paths described in this section allow your applications to continue working and minimize impact on your users, but your users cannot get the full benefits of features in OpenText Documentum CM 6.5 or later versions until the migration is complete.

3.5.1 Setting up a test environment

Before migrating your production system, OpenText recommends that you set up a test environment. Set up an environment that includes the same hardware, RDBMS, and software configurations as your production system, including a copy of your production repository. Setting up a test environment allows you to practice migrating your systems, as well as troubleshoot any migration problems, before committing changes to your production system.

3.5.1.1 Creating the test environment

You cannot create copies of more than one repository in a single new installation if the repositories were created in different installations.

Use the instructions for creating a repository copy on the same operating system as the original repository. The procedure is not supported for moving a repository from one operating system to another.

Before upgrading a repository, create an environment in which to test the upgrade process. To do this, create a new installation using the original Documentum CM Server software version, copy the repository, copy the content files, and upgrade that copy. Perform tests on the copy ensuring to exercise standard functionality and customizations. After the upgraded copy is tested completely, upgrade the original repository.

For example, if you are copying two repositories, Paris and London, that were created in separate Documentum CM Server installations, you need to copy them to separate Documentum CM Server installations. Creating a repository copy requires you to copy the `aek.key` and `dbpasswd.txt` files from the original repository host to the repository copy host, because each repository copy must have access to the `aek.key` and `dbpasswd.txt` files from its original installation.

If you are copying two repositories, Tokyo and Beijing, that were created in the same Documentum CM Server installation, you can create their copies in the same new installation, with the `aek.key` and `dbpasswd.txt` files from the original installation copied to the installation where you create the copies.

"Method 2: Copying a repository" on page 191 in "Migrating Documentum CM Server" on page 185 provides the steps for copying a repository.

3.5.2 Client-first migration

If your system uses only Foundation SOAP API, custom Foundation Java API, or custom WDK clients, you have the option of migrating the client applications first. Refer to the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* for detailed installation or deployment instructions for the client application.

3.5.2.1 OpenText™ Documentum™ Content Management Accelerated Content Services and Branch Office Caching Services version compatibility and migration

When you upgrade the Branch Office Caching Services, update the Branch Office Caching Services version specification in the global registry using Documentum Administrator. For Branch Office Caching Services 6.7 SP2, specify the version as 2.1. For Branch Office Caching Services 7.0 and later, specify the version as 2.3.

3.5.3 Upgrade matrices for Documentum CM Server and related components

This section provides the upgrade matrices for Documentum CM Server and related components. When you plan for upgrade or migration to OpenText Documentum CM 25.x, consider the following points:

- Direct in-place upgrade to OpenText Documentum CM 25.x is supported from OpenText Documentum CM 16.4 Patch 42, but is only supported if the existing operating system, database, and hardware combination is also supported for OpenText Documentum CM 25.x. Otherwise, a migration is required to move to a supported environment.
- For a supported upgrade scenario, all third-party components must also be supported in 6.7 SP2/7.x, 16.x, 20.x, 21.x, 22.x, 23.x, 24.x, and 25.x environments. This only applies to the Documentum CM Server upgrade; it does not imply support for any clients or customizations in the environment to be upgraded.
- Only third-party components supported in OpenText Documentum CM 25.x will work with OpenText Documentum CM 25.x. If the third-party component (such as operating system, database, or application server) does not have a direct upgrade path to the supported version, then direct upgrade for Documentum CM Server is not possible.
- Moving data from one operating system/database to another, is not supported. These scenarios require a fresh installation and engagement with OpenText Global Technical Services.
- Migration of legacy or custom clients is not supported.

Notations used in the tables:

- *Y* - QA tested or paper certified
- *Y** - Read the notes at the end of the table

The upgrade matrix specifically deals with the possible upgrade paths for Documentum CM Server and related server components.

Table 3-7: Upgrade matrix for Documentum CM Server

Documentum CM Server	16.4	16.7	16.7.1	20.2	20.3	20.4	21.1	21.2	21.3	21.4	22.1	22.2	22.4	23.2	23.4	24.2	24.4	25.2	25.4
16.4	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
16.7	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
16.7.1	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
20.2	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
20.3	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
20.4	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
21.1	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
21.2	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
21.3	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
21.4	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
22.1	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y
22.2	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y
22.4	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y
23.2	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y
23.4	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y
24.2	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y
24.4	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y
25.2	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y

Note: To upgrade from a 32-bit Documentum CM Server to a 64-bit Documentum CM Server directly, your underlying operating system and database version must be 64-bit. Otherwise, you must first upgrade the operating system and database before upgrading Documentum CM Server.

Table 3-8: Upgrade matrix for Content Intelligence Services server component

Documentum Content Intelligence Services	Documentum Content Intelligence Services server component							
	7.0 [1] [2]	7.1	7.2	7.3	16.4	16.7	16.7.1	20.2
6.7 SP2	Y	Y	Y	Y	Y	Y	Y	Y
7.0	N	Y	Y	Y	Y	Y	Y	Y
7.1	N	N	Y	Y	Y	Y	Y	Y
7.2	N	N	N	Y	Y	Y	Y	Y
7.3	N	N	N	N	Y	Y	Y	Y
16.4	N	N	N	N	N	Y	Y	Y
16.7	N	N	N	N	N	N	Y	Y
16.7.1	N	N	N	N	N	N	N	Y

[1] Content Intelligence Services 7.0 does not support CenterStage. If you want to migrate Content Intelligence Services data for CenterStage, use Content Intelligence Services 6.7 SP2.
[2] If you want to migrate Content Intelligence Services data to Content Intelligence Services 7.0, you must apply the latest patch for Content Intelligence Services 7.0, that is Patch 04.

Table 3-9: Upgrade matrix for Foundation SOAP API

Foundation SOAP API	Documentum CM Server (Repository)																						
	7.0	7.1	7.2	7.3	16.4	16.7	16.7.1	20.2	20.3	20.4	21.1	21.2	21.3	21.4	22.1	22.2	22.4	23.2	23.4	24.2	24.4	25.2	25.4
00	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
7.0	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
7.1	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
7.2	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
7.3	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
16.4	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
16.7	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
16.7.1	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
20.2	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

Foundation SOAP API	Documentum CM Server (Repository)																						
	7.0	7.1	7.2	7.3	16.4	16.7	16.7.1	20.2	20.3	20.4	21.1	21.2	21.3	21.4	22.1	22.2	22.4	23.2	23.4	24.2	24.4	25.2	25.4
20.3	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
20.4	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
21.1	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
21.2	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
21.3	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
21.4	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
22.1	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y
22.2	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y
22.4	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y
23.2	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y
23.4	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y
24.2	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y
24.4	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y
25.2	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y

Note: Many products consist of multiple installed components (such as WAR file, DAR file, or DocApp). Mixing versions of these components for a particular product version is not supported. OpenText recommends that you use DAR files instead of DocApps whenever possible.

3.6 Planning upgrade for repositories in a federation

A federation is two or more repositories that are bound together to facilitate management of global users, groups, and access control lists (ACLs) in a multi-repository distributed configuration. One repository in the set is the governing repository. The remaining repositories are member repositories.

Keeping objects synchronized in multiple repositories can be time consuming and error-prone when the work is done manually in each repository. A repository federation automates much of the process.

Only certain combinations of different repository versions can work together as a Federation. Plan your upgrade so that all participating repositories are supported.

When you upgrade repositories (that work together as a federation), ensure that the upgraded repository versions (in a nonhomogeneous Federation) can work together as a Federation.

The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more information about configuration requirements in a Federation.

3.6.1 Guidelines for upgrading a distributed configuration

Use these guidelines when deciding how to upgrade a distributed configuration.

3.6.1.1 Repository federations

OpenText Documentum CM supports federations that contain repositories of different versions. In a mixed version environment, upgrade the governing repository first.

3.6.1.2 Repositories with object replication

Upgrade the source repository, then the target repositories. If you have a group of repositories where each repository is both a source and a target, then the upgrade can begin with any of the repositories. This situation can apply, for example, if objects are replicated from repository A to repository B, repository B to repository C, and from repository C to repository A. Although you can replicate between repositories that are different versions, attributes that are only in the newer version cannot be replicated.

3.6.1.3 Repositories with distributed or load-balanced content

Shut down the primary Documentum CM Server and all remote Content Servers. Upgrade the primary Documentum CM Server first, then upgrade the remote Content Servers.

"Upgrading Documentum CM Server in a distributed or load-balanced configuration" on page 53 provides the steps for upgrading Documentum CM Server in a distributed or load-balanced configuration.

3.7 Planning the upgrade or migration of the AEK key from lockbox

You can upgrade the AEK key to a stronger algorithm during the repository upgrade as follows. From Documentum CM Server 16.7, Documentum CM Server does not support lockbox. Install either OpenText Documentum CM 16.4 P10, 7.3 P23, or 7.2 P42 before you proceed to upgrade to 25.x.

Note: During the upgrade process, use the same passphrase for the new AEK key. After the upgrade is complete, change the passphrase. Use `dm_crypto_change_passphrase` to change the passphrase and then run the `dm_crypto_boot` utility with the new passphrase.

For example:

```
dm_crypto_change_passphrase -keyname CSaek -passphrase genuine -newpassphrase glorious
```

Caution

If you select the **Upgrade AEK key** option, it results in changing the AEK key and re-encrypting the repository keys and other related data such as CNT files. Hence, OpenText recommends to take a backup of the AEK key and CNT files before the upgrading the AEK key.

The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about creating strong AEK options.

3.8 Upgrading Documentum CM Server from IPv4 to IPv6

Upgrading Documentum CM Server from IPv4 to IPv6 is supported on both the Windows and Linux operating systems.

To upgrade Documentum CM Server from IPv4 to IPv6 on Linux:

1. Upgrade the Documentum CM Server versions 16.7x or 20.x or 21.x or 22.x or 23.x, 24.x, or 25.x from the IPv4 environment to the Documentum CM Server version 25.4 IPv4 environment.
2. Change the network IP from IPv4 to IPv6 in the Documentum CM Server 25.4 IPv4 machine.
3. Change `HostName` to the IPv4 address of the IPv4 machine and `NewHostName` to the IPv6 address of the IPv6 machine in the `config.xml` file of the migration utility.
4. Run the `MigrationUtil.sh` or `MigrationUtil.csh` file. For more information about the migration utility, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.
5. Restart all the OpenText Documentum CM services.

The preceding list of steps is not required for upgrading Documentum CM Server from IPv4 to IPv6 on Windows.

3.9 Using SSL communication

The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.

Chapter 4

Upgrading Documentum CM Server

This chapter describes how to upgrade from a previous release and how to upgrade repositories to Documentum CM Server 25.x. Always consider upgrading one OpenText Documentum CM component within the context of upgrading the entire OpenText Documentum CM system.

Note: You cannot upgrade to Documentum CM Server 25.x from a version earlier than 6.7 SP2. If your current installation is a version earlier than 6.7 SP2, upgrade it to Documentum CM Server 6.7 SP2 and then to 16.4 Patch 42 before you upgrade to 25.x.

Each step in the upgrade process must be to a system that is fully supported by OpenText Documentum CM. Depending on the Documentum CM Server release from which you are upgrading, you may need to upgrade the operating system or database. The documentation provided by the operating system or database vendor contains information on upgrading those components of the system. After each upgrade step, test the repository to ensure that all functions are normal.

Caution

After upgrading, you cannot revert to previous versions of Documentum CM Server.

4.1 Upgrade checklist

Perform the following tasks for upgrading Documentum CM Server:

1. Review the product *Release Notes*.
2. Review the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.
3. If you are installing the xPlore indexing server, review the *OpenText Documentum xPlore Installation Guide*.
4. If you are using lockbox, then before proceeding with upgrade refer to "Planning the upgrade or migration of the AEK key from lockbox" on page 33.
5. Review "Upgrading to 64-bit Documentum CM Server" on page 41 on what sequence to use in upgrading your installation, especially if you are upgrading from a 32-bit to a 64-bit Documentum CM Server.
6. Ensure that you apply the latest Documentum CM Server patches.

7. Back up the repository. For the steps, refer to the *OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD)*.

8. Optionally, you can take a backup of all users that are part of the `Admin group` and any customized attribute like group_address.

9. Temporarily increase the amount of rollback space available in the RDBMS. The number of rollback segments should be commensurate with the size of the repository and should be in segments of equal size. Refer to the database documentation for the steps.

10. Ensure that you have sufficient disk space on the computer hosting the database.

11. Run the repository consistency checker script and correct any errors you find. The *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* and "Upgrading the Documentum CM Server software" on page 44 provides the steps for running the consistency checker.

12. Ensure that the dm_server_config object is unlocked. "Ensuring that the dm_server_config object is unlocked" on page 40 provides more information.

13. Shut down the repository and all servers running against the repository.

14. Close the Documentum Server Manager user interface.

15. Shut down any local connection brokers.

16. Set the JAVA_HOME and PATH environment variables to the supported JDK version before you start the upgrade process.

    - Windows:
      ```
      mklink %Documentum%\java64\JAVA_LINK <supported version of JDK>
      ```
    - Linux:
      ```
      ln -s $Documentum/java64/JAVA_LINK <supported version of JDK>
      ```

17. On Linux, perform the following tasks:

    - Set the `$DOCUMENTUM` environment variable same as that in the base version.
    - Modify the `$DM_HOME` variable in the installation owner's `.cshrc` or `.profile` file to point to `$DOCUMENTUM/product/25.x`. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more information.
    - Set the `$DOCUMENTUM_SHARED` environment variable same as that in the base version. Do not delete this environment variable.
    - Set the `DM_JMS_HOME` environment variable manually. For example, `$DOCUMENTUM/tomcat`.

- Modify the library path variable in the installation owner's `.cshrc` or `.profile` file to point to the location of the shared libraries required by the server. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more information.
- If you are using Oracle as the database, modify the `$ORACLE_HOME` environment variable to point to the 64-bit libraries.
- Determine the root password. This is the operating system root password. The root password is required to complete the upgrade. Refer to the *Linux* documentation for more information.

18. Determine the installation owner user name and password. Refer to the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*, and consult the database administrator.
19. Determine the names of the repositories you are upgrading.
20. Determine the Documentum CM Server version from which you are upgrading.
21. Upgrade your log4j2. For information, perform the instructions mentioned in the knowledge base article KB19864717 available on OpenText My Support.
22. If your current installation is IPv4 and want to upgrade to IPv6, see "Upgrading Documentum CM Server from IPv4 to IPv6" on page 34.
23. If you are upgrading from earlier versions to Documentum CM Server 25.x, you can change the default passwords of `dmc_wdk_preferences_owner` and `dmc_wdk_presets_owner` users to `webtopUser@12345`. The default password can be changed to a custom password after the upgrade process.
24. If you want to enable HashiCorp Vault, make sure that you store all secret ID information in the HashiCorp Vault server as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* and *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

    Important

    You can use HashiCorp Vault only in the anonymous SSL communication. To upgrade from certificate-based SSL communication, comment the `keystore_file` and `keystore_pwd_file` entries in both the `server.ini` and `docbroker.ini` files. In addition, comment the `dfc.security.ssl.truststore` and `dfc.security.ssl.truststore_password` entries in the `dfc.properties` file.

25. If you want HashiCorp Vault-based SSL communication, you must convert Documentum CM Server from certificate-based SSL communication to non-certificate based SSL communication. Then, upgrade to HashiCorp Vault non-certificate based SSL communication. Finally, create certificates to new HashiCorp Vault AEK key to use certificate-based SSL communication.

4.1.1 Changing the database operating system and version

When migrating your database to a new operating system (host) and database version, complete the database migration first before upgrading Documentum CM Server. After migrating the database, run the Documentum CM Server configuration program to reestablish the repository with the new database instance. Then, upgrade Documentum CM Server to upgrade the entire repository.

Refer to the database vendor documentation for information on migrating the repository database files to a new database instance. The Documentum CM Server configuration program connects Documentum CM Server to the new database host, unless the database connection string, database owner name, or password has changed.

Notes

- While upgrading the Windows operating system, the `\etc\services` file is replaced as a part of the upgrade. Because of this, the entries that were added for the repository before the upgrade is lost. After upgrading the operating system, manually add the repository service entries to the `\etc\services` file.
- After upgrading the Oracle database with Enabled CDB, when the repository is restarted, it will not be able to establish the database connection. You need to modify the `database_conn` name in `server.ini` manually in the Documentum CM Server machine.

4.1.2 Preparing Oracle databases for parallel indexing

Prior to upgrading Documentum CM Server with Oracle databases to create or alter the indexes in parallel, you must edit the `server.ini` file.

If you want to upgrade a repository and also want parallel indexing, then you must edit the `server.ini` file to include the following keys with valid values:

- `db_oracle_dop`
- `db_oracle_index_nologging`
- `db_oracle_online_index`

The *OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD)* and *OpenText Documentum Content Management - Server DQL Reference Guide (EDCCS250400-DRD)* contain more information about the keys and its valid values.

The updated values are reflected in the dm_docbase_config object in the r_module_name (DB_ORACLE_DOP) and r_module_mode (DB_ORACLE_DOP_OTHER_OPTIONS) attributes where DB_ORACLE_DOP has the parallel degree values and DB_ORACLE_DOP_OTHER_OPTIONS updates the value based on the following combination:

- If the value of `db_oracle_index_nologging` is `F` and the value of `db_oracle_online_index` is `T`, then the value is set to `1`.
- If the value of `db_oracle_index_nologging` is `T` and the value of `db_oracle_online_index` is `F`, then the value is set to `2`.
- If the value of `db_oracle_index_nologging` is `T` and the value of `db_oracle_online_index` is `T`, then the value is set to `3`.

Note: After the dm_docbase_config object is updated, whenever indexes are created during the upgrade process, then Documentum CM Server uses these values to create or alter the indexes in parallel. However, if parallel degree values are explicitly given as part of MAKE_INDEX DQL, then the parallel degree values given as part of MAKE_INDEX DQL takes the precedence.

4.1.3 Migrating the database to UTF-8

If the database was installed with a code page other than UTF-8 under a previous version of Documentum CM Server, you do not have to migrate the database to UTF-8 to upgrade Documentum CM Server. However, to use the multilingual functions of Documentum CM Server, migrate the database to UTF-8.

OpenText Documentum CM supports upgrading repositories by using the existing database code page.

- On Oracle, you can migrate existing repositories to Unicode using the tools provided by Oracle. Contact Oracle for any support you require in migrating the database.
- On Microsoft SQL Server, you cannot migrate the database to Unicode.

4.1.4 database_refresh_interval key

During Documentum CM Server installation or upgrade, the change checker process runs once per minute by default. The process updates type caches as types are created or altered. Before you upgrade, ensure that the key is set to 1 minute or delete it from the `server.ini` file.

4.1.5 Ensuring the completion of automatic tasks before upgrading

Ensure that all automatic tasks are completed before shutting down the repository for upgrade; otherwise, unfinished automatic tasks will fail.

Use the following Documentum Query Language (DQL) query to obtain the number of active automatic tasks in the repository:

```
select count(r_object_id) from dmi_workitem where
r_auto_method_id> '0000000000000000' and
r_runtime_state in (0,1)
```

If the query returns a nonzero value, active automatic tasks still must be processed and you must wait for them to complete. If it returns 0, the repository contains no more active automatic tasks, and you can safely stop the repository. If the query returns 0, run the query a few more times to ensure that no new automatic tasks are being generated.

4.1.6 Ensuring that the dm_server_config object is unlocked

If you attempt to upgrade Documentum CM Server and the dm_server_config object is locked, the upgrade may fail. To check if the object is locked, log in to your database as the database owner and use the following SQL query to get the object ID of the server configuration object:

```
SQL> select r_object_id from dm_server_config_s
```

Use the object ID in the following query to verify whether the configuration is locked:

```
SQL> select r_object_id, r_lock_owner from dm_sysobject_s
where r_object_id = '<object ID>'
```

If there is a lock owner, then the object is locked.

To unlock the object, use the following SQL (except for Oracle):

```
SQL> update dm_sysobject_s set r_lock_owner = ' ' set r_lock_machine = ' '
set r_lock_date = ' ' where r_object_id = '<object ID>'
```

For Oracle, use:

```
Oracle> update dm_sysobject_s set r_lock_owner = ' ' set r_lock_machine = ' '
set r_lock_date = null where r_object_id = '<object ID>'
```

Commit the change:

```
SQL> commit
```

Finally, restart the repository.

4.2 Upgrading to 64-bit Documentum CM Server

Upgrading to the 64-bit Documentum CM Server is supported only if there is an upgrade path on the underlying operating system and RDBMS.

If your operating system and database meet the requirements specified in the product *Release Notes*, you can directly upgrade from 32-bit Documentum CM Server 6.7 SP2 or later directly to 64-bit Documentum CM Server 25.x. For this upgrade path, the underlying operating system must be 64-bit.

Use the following approach to upgrade from 32-bit Documentum CM Server 6.7 SP2 or later to 64-bit Documentum CM Server 25.x:

1. Upgrade the operating system to the supported version, if necessary.
2. Upgrade the database, if necessary.
3. Perform one of the following steps depending on the type of database being used:
   - SQL Server: Upgrade or install a 64-bit version of the database client on the Documentum CM Server host machine. When you install the 64-bit database client, copy the DSNs from the 32-bit ODBC driver to the 64-bit driver if used by your database. When you redefine the DSN, use the same level or later level of client library. For more information, see "64-bit ODBC and DSN libraries" on page 42.
   - Oracle: Create an `ORACLE_HOME` environment variable in Windows that points to the location of the 64-bit `TNSNAMES.ORA` file. Copy the entries from the 32-bit `TNSNAMES.ORA` file into the 64-bit `TNSNAMES.ORA` file.
4. Upgrade from 32-bit Documentum CM Server 6.7 SP2 or later to 64-bit Documentum CM Server 25.x.

You may see database connection errors in the repository logs, since the combination of a 32-bit Documentum CM Server and a 64-bit database client is not supported. These errors can be ignored.

During the upgrade from 32-bit to 64-bit, Documentum CM Server, you cannot upgrade the authentication plug-ins that you have installed. You must replace the 32-bit authentication plug-ins with the 64-bit plug-ins. You can find the plug-ins in the `%DM_HOME%\install\external_apps\authplugins` folder.

- Do not probe log files before the entire upgrade is completed. Partial upgrade is not supported. Upgrade the binaries, the connection broker, and the repositories at the same time.
- If the 32-bit Documentum CM Server is installed on a 32-bit operating system, migrate the repository to the 64-bit version of the operating system and then upgrade the Documentum CM Server. If the 64-bit version of the operating system is not supported, you must upgrade the operating system to the supported version before upgrading the Documentum CM Server.

- If you are migrating your database to a new operating system and database version, you must perform the migration before upgrading Documentum CM Server. After completing the database migration, run the Documentum CM Server configuration program to reestablish the repository with the new database instance; then upgrade Documentum CM Server to upgrade the entire repository.

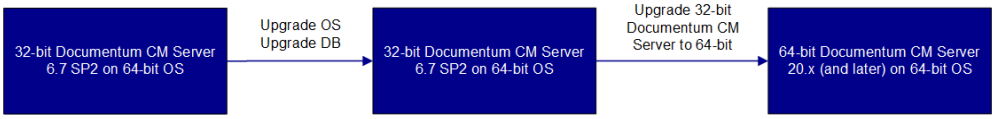


Figure 4-1: Upgrade steps from 32-bit Documentum CM Server to 64-bit Documentum CM Server

4.2.1 64-bit ODBC and DSN libraries

The 64-bit Documentum CM Server requires 64-bit database client libraries for the Oracle database or Microsoft SQL Server. For the Oracle database, update the `ORACLE_HOME` variable to the 64-bit installed path, and `tnsnames.ora` should take the appropriate entries. For Microsoft SQL Server, update the DSN entry from 32-bit to 64-bit and verify that DSN is pointing to the 64-bit SQL libraries.

To migrate the ODBC and DSN libraries from versions for 32-bit Documentum CM Server to versions for the 64-bit Documentum CM Server, follow these steps:

1. Run the 32-bit ODBC DSN utility. Go to `C:\Windows\SysWOW64` and double-click `odbcad32.exe`. The **ODBC Data Source Administrator** dialog box opens.
2. Note down all the DSN entries. These are the 32-bit DSNs present in 32-bit operating system registry.
3. Run the 64-bit ODBC DSN utility. Go to `C:\Windows\System32` and double-click `odbcad32.exe`.
4. In the **ODBC Data Source Administrator** dialog box, on the **System DSN** tab, add the 32-bit DSN entries ensuring that the same values are used as in step 2 and click **OK**.

4.2.2 Errors during upgrade

If you upgrade from 32-bit Documentum CM Server 6.7 SP2 or later to 64-bit Documentum CM Server 25.x, you might encounter errors. During the upgrade, at an intermediate stage where, for example, the 64-bit database client libraries are installed with 32-bit Documentum CM Server and a 64-bit RDBMS is running, the system will be in an unstable state. You can expect to see errors if any of these systems are running. Validation of features or functionality during this intermediate step is not permitted. Continue with the upgrade and run the 64-bit Documentum CM Server installer before testing the system.

When upgrading a repository from 32-bit to 64-bit, Documentum CM Server automatically recompiles the docbasic expressions during their execution. This recompilation occurs because the underlying library changes from 32-bit to 64-bit.

This recompilation process can increase the execution time of the method, which contains these expressions. If a very small method timeout value was specified, the operation can result in a METHOD_TIMEOUT error. However, the method continues running even after the timeout error is reported.

Therefore, when upgrading a repository, watch out for these timeout errors and ensure the proper state of the method before retrying the operation.

4.2.3 Components not supported after upgrade

FAST was the default search engine prior to the OpenText Documentum CM 6.6 Documentum CM Server. FAST is not supported on the 64-bit Documentum CM Server. At a minimum, disable the FAST component on the 64-bit Documentum CM Server. OpenText recommends that you uninstall the FAST component during migration from 32-bit Documentum CM Server 6.7 to 64-bit Documentum CM Server 6.7. OpenText Documentum CM 25.x uses the xPlore search engine. The *OpenText Documentum xPlore Installation Guide* provides information about migrating FAST data to xPlore.

4.2.4 Migrating custom plug-ins

Migrate all 32-bit custom plug-ins to the 64-bit architecture. The 64-bit Documentum CM Server does not support 32-bit custom plug-ins.

4.2.5 Upgrading Documentum CM Server on Red Hat Enterprise Linux 5.x systems

Red Hat Enterprise Linux does not support upgrading the operating system from Linux 5.x to 6.x. If you want to upgrade Documentum CM Server 6.7 SP2 running on a Red Hat Enterprise Linux 5.x system to Documentum CM Server 25.4 that runs on supported Red Hat Enterprise Linux operating system, you must follow the migration procedure described in "Migrating Documentum CM Server" on page 185.

The product *Release Notes* contains the information about the supported versions.

4.3 Upgrading the Documentum CM Server software

The length of time required to upgrade a repository depends on the size of the repository. Allow sufficient time for backing up the repository and performing the upgrade.

Note: If you are using AEK key with lockbox, then ensure that you are using Documentum CM Server 7.2 P42, 7.3 P23 or 16.4 P10, so that you can migrate or upgrade the AEK key for Documentum CM Server 25.x.

To upgrade the Documentum CM Server software:

1. Back up the repository. Several third-party tools are available that you can use.
2. If the repository contains customized repository formats (dm_format objects), back up the customized formats.

   Repository formats are upgraded by the `dm_apply_formats.ebs` script, which reads values from the `formats.csv` file. If the attributes of a format in the repository do not match the format descriptions in the `formats.csv` file, the script overwrites the existing values with the values in the file.
3. Run the Consistency Checker tool.

   Consistency Checker is a script that looks for repository inconsistencies, such as users with nonexistent groups, permissions sets with nonexistent users, and sysobjects that point to nonexistent content files. Fixing inconsistencies in the repository improves the quality of the data in the repository and results in a smoother upgrade. The syntax is:

   ```
   dmbasic -fconsistency_checker.ebs -eEntry_Point -- repository_name
   superuser password
   ```

   - `repository_name` is the name of the repository against which you are running the Consistency Checker tool.
   - `superuser` is the user name of a repository superuser.
   - `password` is the password for the superuser account.

   The results of the Consistency Checker tool are directed to standard output.

4. Fix the inconsistencies reported by the Consistency Checker tool as errors.

   The *OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD)* provides information about the Consistency Checker tool.

5. Upgrade the operating system if necessary.

6. Upgrade the database if necessary.

7. Disable all jobs.

   - On Windows, disable jobs in all repositories on the host.
   - On Linux, disable jobs in all repositories in the installation you are upgrading.

8. (Only for Windows) Install the latest version of Microsoft Visual C++ 2013, 2019, and 2022 Redistributable (64-bit) package before upgrading a repository. This provides the correct operating system runtime libraries for the Documentum CM Server and other utilities.

9. For the upgrade on a Windows host, shut down the repositories and connection brokers.

   a. Click **Start > Programs > Documentum > Server Manager**.
   b. Select the correct Documentum CM Server and click **Stop**.
   c. Click the **Connection Broker** tab.
   d. Select each connection broker.
   e. Click **Stop**.

10. For the upgrade on a Linux host, shut down the repositories and connection brokers.

    a. For each repository, run the dm_shutdown_*<repository>* script, where `repository` is the name of the Documentum CM Server to be stopped.
    b. Stop each connection broker using the dm_stop_docbroker utility.

       The *OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD)* provides the steps for using the dm_stop_docbroker utility.

11. Shut down the application server.

    - To shut down the application server on Windows, stop the service called Java Method Server. Ensure that the application server does not start automatically after a host restart.
    - To shut down the Java Method Server service on Linux, run script `$DM_JMS_HOME/bin/stopMethodServer.sh`.

12. Download and install the supported version of Oracle JDK/OpenJDK version from Oracle JDK/OpenJDK website. The *Oracle JDK and OpenJDK*

documentation contains detailed information. "Using SSL communication" on page 34 provides more details about SSL communication with JDK.

13. If you want to use HashiCorp Vault, perform all the tasks as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*, set the value of `dsis.dctm.vault_type` to `HashiCorp` in the `dsis/application.properties` file, and ensure that Documentum Secret Integration Service (DSIS) is running.
14. Run the Documentum CM Server installation program.
    a. To open the 64-bit Documentum CM Server installer:
       - On Windows, run `serverSetup.exe`.
       - On Linux, run `serverSetup.bin`.

       Note: Before you install Documentum CM Server on Linux, ensure that you have completed the following tasks:

       – Install the Expect version 5.45.4 or earlier script utility.

       – Install the TCL version 8.6.8 or earlier script utility.

       The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more details.

    b. Click **Yes** when the installer displays a message stating that you are trying to upgrade the older version and asks if you want to proceed.
    c. Accept the license agreement and click **Next**.
    d. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.
    e. If you select the **Enable Vault** check box, provide the following information and click **Next**:
       i. **DSIS URL**: Provide a value in the following format:
       ```
       http://localhost:<port mentioned in application.properties>/dsis
       ```
       ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

       Important
       If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

    f. On Windows, provide the installation owner password and click **Next**.
       - If HashiCorp Vault is enabled, the installation owner password is retrieved from the HashiCorp Vault server.

- If HashiCorp Vault is not enabled, type the installation owner password.

g. Browse and specify the directory where the supported version of JDK is installed. Click **Next**.

h. Set the administrator password and specify an available listening port for the embedded application server used by Documentum CM Server and click **Next**.

- **Admin User Password**: Application server password. You must follow the password complexity rules. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about the password complexity rules.
  - If HashiCorp Vault is enabled, then the application server password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, then type the application server password.
- **Listen Port**: The port on which the application server listens for standard administration connections. A total of 20 ports, starting from the one you specify is used by the application server, and all of them must be available. The default port number is 9080. Irrespective of you accepting the default port or choosing another one, do not change this port after the initial configuration.

i. Set the administrator password and specify an available listening port for the embedded application server used by Documentum CM Server and click **Next**.

- **Admin User Password**: Application server password. You must follow the password complexity rules. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about the password complexity rules.
  - If HashiCorp Vault is enabled, then the application server password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, then type the application server password.
- **Listen Port**: The port on which the application server listens for standard administration connections. A total of 20 ports, starting from the one you specify is used by the application server, and all of them must be available. The default port number is 9080. Irrespective of you accepting the default port or choosing another one, do not change this port after the initial configuration.

j. Review the installation summary and click **Install** to begin installation.

k. To open the Documentum CM Server configuration program and configure the repository, select **Configure now** and click **Done**.

Note: When upgrading, if you select this option or the **Configure later** option, you will be prompted to select the connection modes (**Native**, **Secure**, and **Native and Secure**) for the repository upgrade.

During the connection broker upgrade, you will not be prompted to select the connection modes.

l. Recreate the certificates without using the FIPS-compliant `-nomac` option and replace them in the `%DOCUMENTUM%\dba\secure\` folder.

15. Upgrade the connection broker.

a. If you want to manually enable the use of certificates when upgrading the connection broker, follow these steps:

i. Stop the connection broker service.

ii. Add the following properties and modify the `broker.ini` file:

- `secure_connect_mode`
- `keystore_file`
- `keystore_pwd_file`
- `cipherlist`

iii. Add the following properties and modify the `dfc.properties` file:

- `dfc.security.ssl.truststore`
- `dfc.security.ssl.truststore_password`
  - If HashiCorp Vault is enabled, provide the secret ID as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.
  - If HashiCorp Vault is not enabled, type the trust store password.
- `dfc.security.ssl.use_existing_truststore`

iv. Restart the connection broker service.

The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more information about the `broker.ini` and `dfc.properties` properties and the values you can specify with examples.

b. Open the Documentum CM Server configuration program.

c. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

d. If you select the **Enable Vault** check box, provide the following information and click **Next**:

i. **DSIS URL**: Provide a value in the following format:

```
http://localhost:<port mentioned in application.properties>/dsis
```

ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

> **Important**
> If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

e. Select **Connection broker** and click **Next**.

f. On Windows, provide the installation owner password and click **Next**.

- If HashiCorp Vault is enabled, the installation owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the installation owner password.

g. Select **Upgrade a connection broker**.

h. Select the connection broker to upgrade from the list and click **Next**.

i. Complete the configuration, select **Perform additional configuration**, and click **Next**.

16. Upgrade the repository.

a. Click **Upgrade an existing repository**.

b. Select the repository to upgrade from the list and click **Next**.

c. Documentum CM Server 16.7 and later versions do not support lockbox. For more information about creating new AEK key or use existing AEK key, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

d. Type the information for **Connection Broker Port** and **Connection Broker Host** and click **Next**.

e. Select **Connection Mode** for the repository and click **Next**. If you select the **Secure** or **Native and Secure** options, select **Use certificate** on the next page and provide the required details.

If HashiCorp Vault is enabled, to prepare the certificate passwords, the contents of the `broker.pwd` and `server.pwd` files must be updated with the `<secret_name>/<key_name>`. For example:

In the `broker.pwd` file:

```
DOCBROKER_CERT_PASSWORD/<host name of connection broker>
```

In the `server.pwd` file:

```
DOCBASE_CERT_PASSWORD/<repository name>
```

Click **Next**.

f. Select the type of mail server, perform the tasks depending on the mail server you select, and click **Next**. *OpenText Documentum Content*

Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD) contains detailed information.

g. Optional Select **Enable External User Metrics Service** if you want to track the external user transactions and click **Next**.

h. Optional Select the **XML Store** check box if you want OpenText Documentum Content Management (CM) XML Store, specify the following information, and click **Next**:

- **XML Store Host**: Host name of the machine where BaseX server is installed and running.
- **XML Store Port**: Port on which BaseX server is running.
- **XML Store Administrator/Superuser password**: Password of the admin user in BaseX.
  - If HashiCorp Vault is enabled, the XML Store administrator/superuser password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, type the XML Store administrator/superuser password.

i. Specify the data file path for BaseX and click **Next**.

j. Provide the repository owner password and click **Next**.

- If HashiCorp Vault is enabled, the repository owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the repository owner password.

Note: During the upgrade process, a message might appear stating that the repository is not available. Before you click **Yes** in the message box, ensure that the repository is up and running by checking the `<Documentum_Home>\dba\log\<repository>.log` file.

k. After the upgrade completes, select **Finish configuration** and click **Next**.

17. If you upgraded from an installation using FAST full-text indexing, and selected xPlore full-text indexing, restart Documentum CM Server again after you complete the Documentum CM Server configuration.

18. After you complete the Documentum CM Server configuration, create a nonunique index on the `dm_sysobject.r_object_id` and `r_aspect_name` properties by using the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dm_sysobject',
attribute='r_aspect_name',use_id_col=true
```

The inclusion of the `use_id_col` argument set to true automatically causes Documentum CM Server to include the `r_object_id` column in the index.

Note: Before you create the index, verify if it exists already. Check if dm_sysobject has an index on r_aspect_name and r_object_id. If the index does not exist, then create it by using the preceding DQL.

19. If you are upgrading a repository in a distributed environment that uses a Branch Office Caching Services and asynchronous write jobs, create an index on the dmr_content_s (i_parked_state, r_object_id) properties. Use the following MAKE_INDEX command:

```
EXECUTE make_index WITH type_name='dmr_content',
attribute='i_parked_state',use_id_col=true,id_in_front=false
```

Note: When you upgrade Documentum CM Server, the old binaries are not removed. The following binaries are created:

- $DOCUMENTUM/dba/dm_assume_user_cs16.4
- $DOCUMENTUM/dba/dm_change_password_cs16.4.local
- $DOCUMENTUM/dba/dm_change_password_cs16.4.yp
- $DOCUMENTUM/dba/dm_check_password_cs16.4
- $DOCUMENTUM/dba/dm_secure_writer_cs16.4

These files are owned by the installation owner and have their set-user and set-group id bit ON for the installation owner. Documentum CM Server uses the new binaries and does not use the old binaries.

20. After the upgrade is complete:
    - On Linux, log in as the root user, navigate to the $DOCUMENTUM/dba directory and run the dm_root_task_cs16.4 script. On successful execution of the script, the permissions on the dm_secure_writer_cs16.4 file in the $DOCUMENTUM/dba directory and the dmliswap file in the $DOCUMENTUM/product/16.4/install/admin directory are changed.
    - On Linux, delete the $DOCUMENTUM_SHARED/<OLD_JBOSS_HOME> directory.
    - On Windows, delete the %DOCUMENTUM%\<OLD_JBOSS_HOME> directory.
21. Enable all the disabled jobs.
    a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
    b. For each of the previously disabled jobs, right-click the job and select **Properties**.
    c. On the **Properties** page, set the **State** option to Active.
22. On a Windows upgrade, the **Startup Type** is set to Manual for the Documentum Docbase Service *repository name* service. If you want the repository to automatically start after a server reboot, go to **Start > All Programs > Administrative Tools > Services**, and set the **Startup Type** to Automatic.
23. Optionally, run dm_filestore_unique.class in %DM_HOME%\install\tools ($DM_HOME/install/tools in Linux) to create a filestore lock file after upgrade. Processing result (success or failure) can be found in the log file.

24. After upgrade, make sure that you add the backed up list of users to the Admin group. You have to update other groups also if Admin group is member of other groups. In addition, ensure that you manually update the backed up customized attribute. Admin group is recreated as part of the upgrade process, which dissolves all group memberships for `admingroup`. Before the upgrade process, the administrator must document the groups which contain `admingroup` as a member. Similarly, the administrator must document any changes made to the `admingroup` itself. Recreation of memberships must be reapplied after completing the upgrade process.

Note: If you are upgrading Documentum CM Server in a cluster environment and are using a non-default datapath for Documentum CM Server, update `headstart.ebs` to retrieve the correct location object:

```
retrieve,c,dm_location where file_system_path like '%content_storage_01%'
```

4.4 Upgrading Documentum CM Server installed with cluster services

Use the following procedure to upgrade Documentum CM Server installed with Microsoft Cluster Services. This procedure applies to upgrades on active/passive, active/active, single-repository, and multirepository configurations.

To upgrade an active/passive, single-repository cluster:

1. Shut down the Documentum CM Servers on both nodes.

   This shuts down the repository.

2. Shut down both hosts.
3. Restart the first node.

   Do not restart Documentum CM Server on the first node.

4. On the first node, upgrade the Documentum CM Server software. "Upgrading the Documentum CM Server software" on page 44 provides the steps.
5. Upgrade and configure the repository and connection broker.
6. Open the **Services** dialog box and verify that the application server was created correctly.

   If Java Method Server is started, it was created correctly.

7. Test the repository to verify that it is functioning correctly.
8. Shut down the repository on the first node.
9. Shut down the first node.
10. Start the second node.
11. Start the connection broker on the second node.

12. Upgrade the Documentum CM Server software on the second node. "Upgrading the Documentum CM Server software" on page 44 provides the steps.
13. Start the configuration program and select **Custom Configuration**.
14. Select **Upgrade** and the repository to upgrade.
15. When the configuration program reaches the panel on which scripts are run, click **Cancel**.

    Do not run the scripts. The application server is created and the repository is upgraded.
16. To start the application server instance that is running the Java Method Server and OpenText Documentum Content Management (CM) Accelerated Content Services server, restart the Windows hosts after the upgrade is completed.
17. Complete the tasks as described in "Licensing OpenText Documentum CM" on page 59.

4.5 Upgrading Documentum CM Server in a distributed or load-balanced configuration

Use the following procedure to upgrade the Documentum CM Server in a distributed or load-balanced configuration.

To upgrade a distributed or load-balanced configuration:

Note: On Windows, do not reboot the remote hosts by using Terminal Services. Reboot the remote hosts directly from those hosts.

1. On the primary host, upgrade Documentum CM Server, connection brokers, and repository. "Upgrading the Documentum CM Server software" on page 44 contains detailed information to upgrade Documentum CM Server, connection brokers, and repository enabled with and without HashiCorp Vault.
2. On each remote host, upgrade Documentum CM Server and connection broker, but do not install a repository.
3. Run the `cfsConfigurationProgram` to upgrade the content-file server.

   Note: Ensure that you use the same key file name as the primary host.
4. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.
5. If you select the **Enable Vault** check box, provide the following information and click **Next**:

   a. **DSIS URL**: Provide a value in the following format:

```
http://localhost:<port mentioned in application.properties>/dsis
```

b. **DSIS Token**: Provide the `dsis.dctm.token` token value.

> **Important**
> If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

6. On Windows, provide the installation owner password and click **Next**:
   - If HashiCorp Vault is enabled, the installation owner password is retrieved from the HashiCorp Vault server.
   - If HashiCorp Vault is not enabled, type the installation owner password.
7. Select the **Upgrade content-file server** option.
8. Accept the default service name for the new remote Content Server or type a different name.
9. Specify the fully qualified domain name (FQDN) of the remote Content Server host.
10. Specify the password of the primary host machine.
    - If HashiCorp Vault is enabled, password of the primary host machine is retrieved from the HashiCorp Vault server.
    - If HashiCorp Vault is not enabled, type the password of the primary host machine password.
11. If you want to upgrade AEK key, make sure that you update the AEK passphrase to comply with password complexity rules using the following command format:

    ```
    dm_crypto_change_passphrase.exe -keyname <name of aek key> -passphrase <old
    passsphrase> -newpassphrase <new password with complexity rules>
    ```

    For example:

    ```
    dm_crypto_change_passphrase.exe -keyname aek_name -passphrase Password@123 -
    newpassphrase Password@1234567890
    ```

    The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about password complexity rules.

    > **Note:** This step is valid only when upgrading to a repository where HashiCorp Vault is not enabled.

12. If you want to upgrade AEK key in a repository where HashiCorp Vault is enabled, then you must create HashiCorp Vault-based AEK keys.

OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD) contains detailed information.

13. Type the name and port number for the connection broker to which the content-file server instance projects to.

    The default values are `Docbroker` and `1489`. If you are using the default port number, ensure that the next port number (1490) is available for use because the connection broker requires that two ports be reserved. The connection broker is started.

14. Accept the default location of the data directory or browse to a different location.

    The data directory is where content files are stored in the repository.

15. Accept the default location of the share directory or browse to a different location.

    The share directory is where clients, example code, and required libraries are stored.

16. Upgrade is complete.

    To start the application server instance that is running the Java Method Server and Documentum CM Server, perform one of the following actions:

    - On Windows, restart after the installation.
    - On distributed or load-balanced Linux configurations, use Documentum Administrator to set the `Get` method for each component of the distributed or load-balanced store to `Surrogate Get`.

17. If required, modify the `dm_server_config` object to specify only the `app_server_name` and `app_server_uri` entries that are relevant to the remote Content Server.

    Note: The remote Content Server upgrade clones a copy of the `dm_server_config` object from the original repository. Hence, unnecessary attribute values might have been copied over. For example, if an index agent and Business Process Engine are in the original repository, you might have entries for them that point to the original host machine on the remote host. Remove any of these attributes if they are not applicable to the new remote Content Server upgrade.

18. To create an `acs config` object in the repository for each of the Accelerated Content Services servers installed with each remote Content Server (that is, if there are three remote Content Servers, create three `acs config` objects), run one of the following scripts on each remote Content Server host:

    - Windows: `%DM_HOME%\install\admin\dm_acs_install.ebs`
    - Linux: `$DM_HOME/install/admin/dm_acs_install.ebs`

    The syntax is as follows:

```
dmbasic -f dm_acs_install.ebs -e Install -- <repository_name> <user_name>
<password> <acs_name> <server_config_name> <Java_method_server_port> <acs_protocol>
<CleanupCacheAcsObject>
<CacheAcsDescriptionFile> <HostName>
```

"Parameters required by dm_acs_install.ebs script" on page 56 describes the parameters. The `acs config` object is created in `server config mode` and uses the network locations, connection broker projection targets, and stores from the associated `server config` object. If you must change the mode to `acs config mode`, in which you manually set network locations, connection broker projection targets, and stores, use Documentum Administrator to change the mode and create the manual settings.

Note: Do not use the OpenText Documentum CM API or DQL to modify the new `acs config` object.

Table 4-1: Parameters required by dm_acs_install.ebs script

Parameter	Description and values
acs_name	Object name of the `acs config` object you are creating. This name can be any arbitrary name, but the name must be unique among the object names of `acs config` objects and the `server config` objects of both the primary Documentum CM Server and any remote Content Server.
acs_protocol	Communication protocol used by the Accelerated Content Services server. Valid values are `http` and `https`.
CacheAcsDescriptionFile	File to store object dump of candidate `dm_bocs_config` objects. See `CleanupCacheAcs` description.
CleanupCacheAcsObject	Set to F. **Note:** T was only required when upgrading from a previous version from which upgrading is no longer supported.
HostName	Fully-qualified domain name of host. This value is used to set the `acs_url` attribute of the `dm_acs_config` used by the server named in `dm_server_name`.
Java_method_server_port	Port where the application server on the remote Content Server host listens, which was provided during remote Content Server installation. Do not change this port number after the initial configuration.
password	Password for the superuser account.

Parameter	Description and values
repository_name	Name of the repository served by the remote Content Server and its Accelerated Content Services server, where the `acs config` object is being created.
server_config_name	Object name of the `server config` object of the remote Content Server.
user_name	Username of a user with superuser privileges, for example, the installation owner.

19. If the remote Content Servers are installed in a different file-system path from the primary Documentum CM Server, create new site-specific location objects for locations that are new in the upgraded repository.

    a. Using Documentum Administrator, connect to the repository.

    b. Create site-specific `dm_dba` and `auth_plugin` location objects that contain the locations on each of the remote sites of `$DOCUMENTUM/dba` (Linux) or `%DOCUMENTUM%\dba` (Windows) and the authentication plug-in.

    c. In the server config object for the remote Content Server, set the `auth_plugin_location` and `dba_location` to the location objects you created.

20. Start the application server.

Note: Ensure that you enable the Trusted Server Privilege and Trusted Login for all the Documentum CM Server related `DFC privileged clients` using Documentum Administrator to avoid authentication issues in multi-Documentum CM Server environments.

4.5.1 Upgrading the Branch Office Caching Services server

A Branch Office Caching Services server is a caching server. It is a separate, optional product with its own installer. It is not installed with Documentum CM Server. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more information about Branch Office Caching Services.

The Branch Office Caching Services server is one component of a distributed configuration. When upgrading the Documentum CM Server in a distributed configuration, you may want to upgrade the Branch Office Caching Services server as well to use latest features available in Branch Office Caching Services/Accelerated Content Services.

To upgrade the Branch Office Caching Services server:

1. Log on as the owner of the existing Branch Office Caching Services installation.

2. Download and extract the compressed distribution file to a temporary location on the Branch Office Caching Services server host.

3. Stop the current Branch Office Caching Services server and its components.

4. Follow the installation steps provided in the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* to install Branch Office Caching Services.

5. Migrate `acs.properties` from the previous version's location to the new location.

6. Complete the tasks as described in "Licensing OpenText Documentum CM" on page 59.

4.5.2 Upgrading the OpenText™ Documentum™ Content Management Messaging Service server

In a distributed configuration, the OpenText Documentum Content Management (CM) Messaging Service server facilitates the precaching for Branch Office Caching Services server and asynchronous write operations for remote users. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more information about Messaging Service. You can only upgrade Messaging Service from 7.0 to 16.7 because in OpenText Documentum CM 7.0, the Messaging Service installation was integrated with Documentum CM Server.

To upgrade the Messaging Service server:

If you are upgrading from 6.7 SP2 to 25.x, then ensure that you complete this procedure.

1. Ensure that you have Documentum CM Server 7.0 and Messaging Service 7.0 installed in your environment.

2. Ensure that the connection broker and the global repository are configured for Documentum CM Server 25.x.

3. Upgrade Documentum CM Server 7.0 to 25.4. For the steps, see "Upgrading the Documentum CM Server software" on page 44.

4. Upgrade the connection broker and global repository to 25.4.

5. Upgrade Messaging Service to 25.4.

    a. Use the Documentum CM Server configuration program to upgrade Messaging Service:

        - Linux: Run `$DM_HOME/install/Server_Configuration_Program.sh` and select **Documentum Messaging Service (DMS)**.

- Windows: Click **Start > All Programs > Documentum > Documentum Server Manager** and on the **Utilities** tab, click **Server Configuration**, and then select **Documentum Messaging Service (DMS)**.

b. Complete the upgrade as instructed.

6. Complete the tasks as described in "Licensing OpenText Documentum CM" on page 59.

During the Messaging Service upgrade, the old Messaging Service installation is deleted from JBoss and Messaging Service 25.x is installed in a separate instance of Tomcat (`dms_tomcat`).

4.6 Post-upgrade tasks

This section provides the information about the post-upgrade tasks.

4.6.1 Licensing OpenText Documentum CM

4.6.1.1 Procuring license file from OpenText

Procure the license file from OpenText as described in the *Obtain the license key* section in OpenText Documentum Content Management License Management (https://support.opentext.com/csm?id=kb_article_view&sysparm_article=KB0834991).

4.6.1.2 Configuring OTDS and license

This section provides the information about configuring OTDS and license.

- For information about configuring OTDS using an automated method and configuring license using a manual method, see "To configure OTDS using an automated method and to configure license using a manual method:" on page 59.
- For information about configuring OTDS and license using a manual method, see "To configure OTDS and license using a manual method:" on page 63.

To use these instructions, ensure that you have upgraded OTDS. For more information about upgrading, see *OpenText Directory Services - Installation and Administration Guide (OTDS250400-IWC)*.

To configure OTDS using an automated method and to configure license using a manual method:

1. Sign in to the OTDS Admin website using the following information:

   - URL: URL to access the OTDS Admin website.

     <fully qualified domain name of server>:*<web application server port number>*/otds-admin

   - User name: OTDS Admin user name.

For example: `otadmin@otds.admin`

- Password: OTDS Admin password.

2. Synchronize the resources to the Documentum CM repository using the following steps:

   a. Click **Resources**.
   b. Click **<***your resource name***> > Actions > Consolidate**.

      For example: Your resource name can be `otdctmresource`.

3. Import the license file in OTDS using the following steps:

   a. On the **License Keys** page, click **Add**.
   b. On the **General** tab, provide values for the following fields:

      - **License Key Name**: Unique name.

        For example: `otdctmlicense`

      - **Resource ID**: License linked to the resource.

   c. On the **License Key** tab, click **Get License File**, browse and select the license file.
   d. Click **Save**.

4. Create a `businessadmin` user in the `otds.admin` partition using the following steps:

   a. Click **Partitions**.
   b. Click **otds.admin > Actions > View Members.**.
   c. Click **Add > New User**.
   d. On the **General** page, in the **User Name** box, type a name for this user as `businessadmin`.
   e. On the **Account** page, in the **Password Options** area, do the following:

      i. Click **Do not require password change on reset** from the list.
      ii. Clear the **User cannot change password** check box, if selected.
      iii. Select the **Password never expires** check box and click **Save**.

Additional information and tasks

Documentum CM client

Create OTDS users with the user name as `d2_mail_manager` and `d2_wf_notification_user` and keep the passwords as blank in a new non-synchronized partition which is not associated to any resources in OTDS.

By default, OTDS is enabled for client configuration. If you disable OTDS, add another user with the user name as `install_owner_user` to the same partition with the password as blank.

In the **Password Options** area, click **Do not require password change on reset** from the list, and do the following:

- Select the **User cannot change password** check box.
- Select the **Password never expires** check box.

This is applicable only for the system account user partition.

Workflow Designer

If you want to use Workflow Designer with the skip SSO feature, only a user with the `install_owner` privilege can access without a license.

Advanced Workflow

Advanced Workflow is available with advanced license or as an add-on. As a user, you can build processes using Advanced Workflow but to install these processes, the xDA Documentum CM repository endpoint user must have advanced Documentum CM or an add-on license.

To start a workflow at runtime from any Documentum CM client components, you must have advanced Documentum CM or an add-on license and the required transaction capability. The transaction counter increments at runtime when a user creates a new instance of workflow irrespective of the state of the workflow.

Reports

Create an OTDS user with the user name as `dctmreports` and keep the password as blank.

In the **Password Options** area, click **Do not require password change on reset** from the list, and do the following:

- Select the **User cannot change password** check box.
- Select the **Password never expires** check box.

OpenText Documentum CM for Microsoft 365, OpenText Documentum CM Online Editing Service, and Notification Service

Create an OTDS user with the user name as `M365_SERVICE` with the password as `Xecmserviceuser@123`. The password is case-sensitive.

In the **Password Options** area, click **Do not require password change on reset** from the list, and do the following:

- Clear the **User cannot change password** check box.
- Select the **Password never expires** check box.

Documentum Archive Services for SAP Solutions

Create an OTDS user with the user name as `installownerusername` with the password as `installownerpassword`. This is a service account.

The system automatically changes the password after the service is started.

5. Add the `businessadmin` user to the `otdsbusinessadmins` group in OTDS using the following steps:

   a. Click **Users & Groups**, and select the **Groups** tab.
   b. In the **Search** box, type `otdsbusinessadmins` to find the `otdsbusinessadmins@otds.admin` group.
   c. On the **Groups** tab, click **Actions > Edit Membership**.
   d. On the **otdsbusinessadmins@otds.admin** page, on the **Members** tab, click **Add Member**.
   e. In the **Search** box, type `businessadmin` to find the `businessadmin@otds.admin` member.
   f. Select the **businessadmin@otds.admin** check box, and click **Add Selected**.

6. In the Documentum CM Server machine, run the following command in IAPI to create the `dm_otds_license_config` object:

```
create,c,dm_otds_license_config
set,c,l,otds_url
<otds_url_including_rest>
set,c,l,license_keyname
<license_keyname>
set,c,l,business_admin_name
<business_adminname>
set,c,l,business_admin_password
<password>
save,c,l
```

   For example:

```
create,c,dm_otds_license_config
set,c,l,otds_url
http://documentumcm:8080/otdsws/rest
set,c,l,license_keyname
otdctmlicense
set,c,l,business_admin_name
businessadmin
set,c,l,business_admin_password
Password-1234567890
save,c,l
```

   Notes

   - Alternatively, you can create the `dm_otds_license_config` object using the Documentum Administrator graphical user interface.

     For instructions, see *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)*.

   - If you modify the `dm_otds_license_config` object after the first time, you must run the `apply,c,NULL,FLUSH_OTDS_CONFIG` command in IAPI.

7. Allocate a license in OTDS to a partition using the following steps:

   a. Click **Partitions > <***your desired partition***> > Actions > Allocate to License**.
   b. On the **Allocate to License** page, click the relevant counter from the list.

      You can also allocate the license to users and groups. When you allocate a license, ensure that you allocate the relevant counter to a user or group.

c. Click **Allocate to License**.

Notes

- If you modify the allocated license file after the initial deployment, you must restart OTDS.
- You can allocate users to your license any time, but a user must exist before you can allocate the user to a license. The changes to the allocation, deallocation, and revocation take effect after 24 hours for releases prior to and including the 24.4 release.
  - For the 25.2 release, run the following command in IAPI to get the allocation, deallocation, revocation, or deletion with immediate effect:

    ```
    apply,c,NULL,FLUSH_JMS_OTDS_CACHE
    ```

  - From the 25.4 release, run the following command in IAPI to get the allocation, deallocation, revocation, or deletion with immediate effect:

    ```
    apply,c,NULL,FLUSH_OTDS_CACHE
    ```

8. In the Documentum CM Server machine, open the `otdsauth.properties` file in the `$DM_HOME\OTDSAuthLicenseHttpServerBin\config` folder and verify if information for `certificate`, `otds_rest_credential_url`, `otds_rest_ticket_url`, and `admin_username` are updated.
9. Sign in to a deployed application (for example, Documentum Administrator) with any licensed user to verify the license configuration.

   Ensure that the user authentication is successful.

To configure OTDS and license using a manual method:

1. Sign in to the OTDS Admin website using the following information:
   - URL: URL to access the OTDS Admin website.

     <fully qualified domain name of server>:*<web application server port number>*/`otds-admin`
   - User name: OTDS Admin user name.

     For example: `otadmin@otds.admin`
   - Password: OTDS Admin user password.
2. Create a non-synchronized user partition in OTDS using the following steps:
   a. Click **Partitions > Add > New Nonsynchronized User Partition**.
   b. In the **Name** box, type a name for your user partition.

      For example: `otdctmpartitions`
   c. Click **Save**.

For information to create a synchronized user partition in OTDS, see *OpenText Directory Services - Installation and Administration Guide (OTDS250400-IWC)*.

3. Create a synchronized resource in OTDS using the following steps:

   a. Click **Resources > Add**.
   b. On the **General** page, do the following:

      i. In the **Resource name** box, type a name for the resource.

         For example: `otdctmresource`

      ii. In the **Description** box, type a description for the resource.
      iii. On the **Synchronization** tab, select the **User and group synchronization** check box and click **REST(Generic)** for **Synchronization connector**.
      iv. Click **Next**.

   c. On the **Resources > <***your resource name***> > Actions** page, select **Properties**.

      For example: Your resource name can be `otdctmresource`.

      i. On the **<***your resource name***>** page, select the **Connection Information** tab.
      ii. On the **Connection Information** page, provide the value for the following fields:

         - **Base URL**: URL endpoint for user or group provisioning REST API.

           Use the following format:

           `http://<host name>:<port>/dmotdsrest`

           For example: `http://dcs-pg-jms-service:9080/dmotdsrest`

         - **Username**: Installation owner user name for the repository.

           Use the following format:

           `<repository name>\<installation owner user name>`

           For example: `docbase1\dmadmin`

         - **Password**: Installation owner password for the repository.

   d. Click **Test Connection**.
   e. On the **User Attribute Mappings** tab, click **Reset to Default**.
   f. For **User Attribute Mappings**, add the `client_capability` attribute with `Format` value of `2`.

      Add the `default_folder` attribute with `OTDS Attribute` value of `cn` and `Format` value of `/%s`.
   g. Retain the default value for all other settings.
   h. Click **Next**.
   i. On the **Group Attribute Mappings** tab, click **Reset to Default**.
   j. Click **Save**.

4. Click **Access Roles** and go to **Access to <***your resource name***>** (for example, `otdctmresource`).

   a. Click **Actions** and select **Include Groups**.
   b. Click **Actions** and select **View Access Role Details**.
   c. On the **User Partitions** tab, add the partition you created.
   d. Click **Save**.

5. Click **Resources > <***your resource name***> > Actions > Consolidate** to synchronize the members to your repository.

6. Click **OAuth clients** and create an OAuth client.

   a. For **Redirect URLs**, add the following to the **Redirect URLs** list:

      - `<Ingress URL>/D2/d2_otds.html`
      - `<Ingress URL>D2/OTDSLogoutResponse.html`
      - `<Ingress URL>/D2-Config/d2config_otds.html`
      - `<Ingress URL>/D2-Config/OTDSLogoutResponse.html`
      - `<Ingress URL>D2-Smartview/ui`
      - `<Ingress URL>oes-connector`
      - `<Ingress URL>AdminConsole`
      - `<Ingress URL>d2-rest`
      - `<Ingress URL>`

      Note: If you have disabled OTDS for client configuration, do not add the following URLs to the **Redirect URLs** list:

      - `<Ingress URL>/D2-Config/d2config_otds.html`.
      - `<Ingress URL>/D2-Config/OTDSLogoutResponse.html`.

   b. Click **Save**.

7. Click **Auth Handlers**, select **http.negotiate**, click **Action**, and select **Disable**.

8. Create roles using the following steps:

   a. Click **Partitions > <***your desired partition***> > Actions > View Members**.
   b. On the **Roles** tab, click **Add > New Role**.
   c. Add the following roles:

      - Client Capabilities: `Client_Consumer`, `Client_Contributor`, `Client_Coordinator`, and `Client_System_Administrator`.
      - User Privileges: `privilege_createtype`, `privilege_createcabinet`, `privilege_creategroup`, `privilege_sysadmin`, and `privilege_superuser`.

Note: The role name is case-sensitive.

d. Go to **Application Roles** to view the list of added roles.

9. Import the license file in OTDS using the following steps:

   a. On the **License Keys** page, click **Add**.
   b. On the **General** tab, provide values for the following fields:

      - **License Key Name**: Unique name.

        For example: `otdctmlicense`

      - **Resource ID**: License linked to the resource.

   c. On the **License Key** tab, click **Get License File**, browse and select the license file.
   d. Click **Save**.

10. Create a `businessadmin` user in the `otds.admin` partition using the following steps:

    a. Click **Partitions**.
    b. Click **otds.admin > Actions > View Members.**.
    c. Click **Add > New User**.
    d. On the **General** page, in the **User Name** box, type a name for this user as `businessadmin`.
    e. On the **Account** page, in the **Password Options** area, do the following:

       i. Click **Do not require password change on reset** from the list.
       ii. Clear the **User cannot change password** check box, if selected.
       iii. Select the **Password never expires** check box and click **Save**.

Additional information and tasks

Documentum CM client

Create OTDS users with the user name as `d2_mail_manager` and `d2_wf_notification_user` and keep the passwords as blank in a new non-synchronized partition which is not associated to any resources in OTDS.

By default, OTDS is enabled for client configuration. If you disable OTDS, you must add another user with the user name as `install_owner_user` to the same partition with the password as blank.

In the **Password Options** area, click **Do not require password change on reset** from the list, and do the following:

- Select the **User cannot change password** check box.
- Select the **Password never expires** check box.

This is applicable only for the system account user partition.

Workflow Designer

If you want to use Workflow Designer with the skip SSO feature, only a user with the `install_owner` privilege can access without a license.

Advanced Workflow

Advanced Workflow is available with advanced license or as an add-on. As a user, you can build processes using Advanced Workflow but to install these processes, the xDA Documentum CM repository endpoint user must have advanced Documentum CM or an add-on license.

To start a workflow at runtime from any Documentum CM client components, you must have advanced Documentum CM or an add-on license and the required transaction capability. The transaction counter increments at runtime when a user creates a new instance of workflow irrespective of the state of the workflow.

Reports

Create an OTDS user with the user name as `dctmreports` and keep the password as blank.

In the **Password Options** area, click **Do not require password change on reset** from the list, and do the following:

- Select the **User cannot change password** check box.
- Select the **Password never expires** check box.

OpenText Documentum CM for Microsoft 365, OpenText Documentum CM Online Editing Service, and Notification Service

Create an OTDS user with the user name as `M365_SERVICE` with the password as `Xecmserviceuser@123`. The password is case-sensitive.

The password is updated when the notification service is started.

In the **Password Options** area, click **Do not require password change on reset** from the list, and do the following:

- Clear the **User cannot change password** check box.
- Select the **Password never expires** check box.

Documentum Archive Services for SAP Solutions

Create an OTDS user with the user name as `installownerusername` with the password as `installownerpassword`. This is a service account.

The system automatically changes the password after the service is started.

11. Add the `businessadmin` user to the `otdsbusinessadmins` group in OTDS using the following steps:

    a. Click **Users & Groups**, and select the **Groups** tab.

b. In the **Search** box, type `otdsbusinessadmins` to find the `otdsbusinessadmins@otds.admin` group.

c. On the **Groups**, click **Actions > Edit Membership**.

d. On the **otdsbusinessadmins@otds.admin** page, on the **Members** tab, click **Add Member**.

e. In the **Search** box, type `businessadmin` to find the `businessadmin@otds.admin` member.

f. Select the **businessadmin@otds.admin** check box, and click **Add Selected**.

12. In the Documentum CM Server machine, run the following command in IAPI to create the `dm_otds_license_config` object:

```
create,c,dm_otds_license_config
set,c,l,otds_url
<otds_url_including_rest>
set,c,l,license_keyname
<license_keyname>
set,c,l,business_admin_name
<business_adminname>
set,c,l,business_admin_password
<password>
save,c,l
```

For example:

```
create,c,dm_otds_license_config
set,c,l,otds_url
http://documentumcm:8080/otdsws/rest
set,c,l,license_keyname
otdctmlicense
set,c,l,business_admin_name
businessadmin
set,c,l,business_admin_password
Password-1234567890
save,c,l
```

Notes

- Alternatively, you can create the `dm_otds_license_config` object using the Documentum Administrator graphical user interface.

  For instructions, see *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)*.

- If you modify the `dm_otds_license_config` object after the first time, you must run the `apply,c,NULL,FLUSH_OTDS_CONFIG` command in IAPI.

13. Allocate a license in OTDS to a partition using the following steps:

a. Click **Partitions > <***your desired partition***> > Actions > Allocate to License**.

b. On the **Allocate to License** page, click the relevant counter from the list.

Note: You can also allocate the license to users and groups. When you allocate a license, ensure that you allocate the relevant counter to a user or group.

c. Click **Allocate to License**.

Notes

- If you modify the allocated license file after the initial deployment, you must restart OTDS.
- You can allocate users to your license any time, but a user must exist before you can allocate the user to a license. The changes to the allocation, deallocation, and revocation take effect after 24 hours for releases prior to and including the 24.4 release.
  - For the 25.2 release, run the following command in IAPI to get the allocation, deallocation, revocation, or deletion with immediate effect:

    ```
    apply,c,NULL,FLUSH_JMS_OTDS_CACHE
    ```

  - From the 25.4 release, run the following command in IAPI to get the allocation, deallocation, revocation, or deletion with immediate effect:

    ```
    apply,c,NULL,FLUSH_OTDS_CACHE
    ```

14. Import all the inline and Lightweight Directory Access Protocol (LDAP) users to OTDS:

    - On Windows:

      In the Documentum CM Server machine, copy the `dfc.properties` file to the `$DOCUMENTUM\Shared` folder. At the command prompt, go to the `$DOCUMENTUM\Shared` folder, and then run the following command:

      ```
      java --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/
      java.io=ALL-UNNAMED --add-opens=java.base/java.util=ALL-UNNAMED --add-
      opens=java.base/java.util.concurrent=ALL-UNNAMED --add-opens=java.rmi/
      sun.rmi.transport=ALL-UNNAMED --add-exports=java.base/
      sun.security.provider=ALL-UNNAMED --add-exports=java.base/
      sun.security.pkcs=ALL-UNNAMED --add-exports=java.base/sun.security.x509=ALL-
      UNNAMED --add-exports=java.base/sun.security.util=ALL-UNNAMED --add-
      exports=java.base/sun.security.tools.keytool=ALL-UNNAMED -
      cp .;dfc.jar;dfc.properties;* com.documentum.fc.tools.MigrateInlineUsersToOtds
      <repository name> <installation owner user name> <installation owner password>
      <non-synchronized partition name>
      ```

    - On Linux:

      In the Documentum CM Server machine, copy the `dfc.properties` file to the `$DOCUMENTUM\dfc` folder. At the command prompt, go to the `$DOCUMENTUM\dfc` folder, and then run the following command:

      ```
      java --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/
      java.io=ALL-UNNAMED --add-opens=java.base/java.util=ALL-UNNAMED --add-
      opens=java.base/java.util.concurrent=ALL-UNNAMED --add-opens=java.rmi/
      sun.rmi.transport=ALL-UNNAMED --add-exports=java.base/
      sun.security.provider=ALL-UNNAMED --add-exports=java.base/
      sun.security.pkcs=ALL-UNNAMED --add-exports=java.base/sun.security.x509=ALL-
      UNNAMED --add-exports=java.base/sun.security.util=ALL-UNNAMED --add-
      exports=java.base/sun.security.tools.keytool=ALL-UNNAMED -
      cp .:dfc.jar:dfc.properties:* com.documentum.fc.tools.MigrateInlineUsersToOtds
      <repository name> <installation owner user name> <installation owner password>
      <non-synchronized partition name>
      ```

15. Configure the OTDS authentication using the following steps:

a. In the Documentum CM Server machine, open the `otdsauth.properties` file in the `$DM_HOME\OTDSAuthLicenseHttpServerBin\config` folder.

b. Update the values for the following variables:

- `certificate`

  Run the following URL to obtain the certificate value:

  ```
  http://<OTDS server name>:8080/otdsws/rest/systemconfig/certificate_content
  ```

- `otds_rest_credential_url`

  For example: `otds_rest_credential_url=http://192.168.2.105:8080/otdsws/rest/authentication/credentials`

- `otds_rest_ticket_url`

  For example: `otds_rest_ticket_url=http://192.168.2.105:8080/otdsws/rest/authentication/resource/validation`

- `admin_username`

  For example: `admin_username=dmadmin`

16. To verify the license configuration, sign in to any deployed application (for example, Documentum Administrator) with any licensed user.

    Ensure that user authentication is successful.

4.6.1.3 Creating new users, allocating license, and applying roles in OTDS

1. Go to **Partitions > <*partition name*> > Actions > View Members > Add > New user**.
2. Create a new user with a desired name (for example, `otdctmuser`), and set all the attributes including password.
3. Click **Save**.
4. Select the user you created and click **Actions > Allocate to License**.
5. On the **Allocate to License** dialog box, select the relevant counter and click **Allocate to License**.
6. Select the user you created and click **Actions > Edit Application Roles**.
7. Click **Assign Roles** and select a desired role for the user.

   For more information about the list of roles, see step 8.c.

   Note: Ensure `da_privilege_enabled=T` and `lss_cc_enabled=T` are added in the `<Java Method Server Home>/webapps/dmotdsrest/WEB-INF/classes/dmotds.properties` file in the Documentum CM Server machine.

8. Click **Add Selected** and then click **Close**.

4.6.1.4 Troubleshooting license configuration

The following table describes the license-related errors captured in the `$DOCUMENTUM/dba/log/otdsauth.log` file.

Error code	Description	Solution
`DM_LICENSE_E_NO_LICENSE_CONFIG`	The license configuration is not created in the repository.	Ensure that you activate the license from IAPI or Documentum Administrator.
`DM_LICENSE_E_CONFIG_MISSING_PARAMS`	One of the following mandatory parameters is not available: OTDS URL, or OTDS business administrator credentials, or License key	Ensure that you have provided valid values in IAPI or Documentum Administrator.
`DM_LICENSE_E_SERVER_NOTREACHABLE`	The OTDS URL is not reachable.	Ensure that the OTDS installation is active and reachable.
`DM_LICENSE_E_BAD_ADMIN_CRED`	OTDS business administrator credentials are incorrect or locked.	Before you activate the license, ensure that you have provided valid values in IAPI or Documentum Administrator.
`DM_LICENSE_E_REQ_BUSINESS_ADMIN`	The OTDS business administrator user is not added to the `otdsbusinessadmins` group in OTDS.	Ensure that you add the business administrator user to the `otdsbusinessadmins` group in OTDS.
`DM_LICENSE_E_NO_LICENSE`	The license key is not configured with the license file in OTDS.	Ensure that you upload the license file in OTDS to generate the license key and provide the correct license key.
`DM_LICENSE_E_INVALID_LICENSE`	The license file is invalid.	Ensure that you have uploaded a valid license file in OTDS.
`DM_LICENSE_E_USER_NOT_FOUND_OR_DUPLICATE`	The user is not found in OTDS or the user is not unique in OTDS.	Ensure that the user exists in OTDS and is unique.
`DM_LICENSE_E_USER_NO_LICENSE_ALLOCATED`	The user is not allocated with a counter.	Ensure that you allocate a counter to the user in OTDS.
`DM_LICENSE_E_USER_NO_ACCESS`	The user is not allocated to the relevant counter or all the licenses for users or transactions are consumed.	Ensure that you allocate the user to the relevant counter in OTDS.

Error code	Description	Solution
DM_LICENSE_E_ UNEXPECTED_ERROR	There is an unexpected error in the licensing code.	Analyze the otdsauth.log file to troubleshoot the issue.
DM_LICENSE_E_ SYSTEMACCT_MISUSE	When a system account user is allocated to any other counters.	Remove the SYSTEMACCT or other counters.
DM_LICENSE_E_ SERVICEACCT_MISUSE	When a service account user is allocated to any other counters.	Remove the SERVICEACCT or other counters.

4.6.2 Improving performance after upgrade

To avoid performance degradation after upgrading to Documentum CM Server 25.4, you must configure the values of the following two parameters:

- Number of method server threads: The method_server_threads parameter affects the number of worker threads. Depending on the number of dmbasic jobs, you can tune this value. For all operating systems, in the server.ini file, set method_server_threads to 3.
- Java virtual machine (JVM) heap memory: The java.ini file specifies the options to the JVM, which is used by the dmbasic method server. This includes settings for the minimum and maximum heap memory for the JVM. Depending on your environment, you can tune this heap memory in the java.ini file:

  On Windows, set the following value:

  ```
  JAVA_OPTIONS=" -Xcheck:jni -XX:+RestoreMXCSROnJNICalls -Xms256m -Xmx512m"
  ```

  Xms specifies the startup heap value and Xmx specifies the maximum heap size for the Java heap. These values should be set or tuned cautiously to avoid allocating too much or too little heap memory. Allocating too much heap memory reduces the system's memory for other processes. Allocating too little causes Java programs to crash with heap errors. -Xcheck:jni is used for debugging purpose only.

4.6.3 Extending the Oracle tablespace size

After you upgrade Documentum CM Server from 6.7 SP2 and later to 25.4, you must manually extend the Oracle tablespace size based on your requirements. This is because the default Oracle tablespace size, which is set to 2 GB, might be insufficient and may lead to tablespace-related issues in OpenText Documentum CM 25.x.

4.6.4 Configuring operation mode

OpenText Documentum CM is designed to run as schema owner (Documentum CM Server database user) during both administration and daily operation modes. The privileges are categorized as schema owner (administration) and the normal database user with restricted privileges (operation mode). *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more details.

4.6.5 Reinstalling OpenText™ Documentum™ Content Management client libraries

OpenText Documentum Content Management (CM) client JAR files go missing on Documentum CM Server after Documentum CM Server is upgraded to 20.4 and later versions. This occurs because the Documentum CM Server upgrade operation creates a new JBoss folder, where the existing OpenText Documentum CM client JAR files are not preserved. Therefore, you must reinstall the OpenText Documentum CM client JAR files after upgrading the Documentum CM Server. The *OpenText Documentum Content Management - Client Installation Guide (EDCCL250400-IGD)* provides the steps for installing the OpenText Documentum CM client.

4.6.6 Rebuilding the database views

DQL statements are translated into SQL statements that query the database views. Documentum CM Server creates and maintains these views, which in some rare instances, may get corrupted. In such cases, after completing the upgrade process, you need to rebuild the database views. The `views_valid` attribute indicates the status of the views. It is part of `dm_type` object, so there is one `views_valid` attribute per OpenText Documentum CM object type. By setting the value of this attribute to false (0), you can force the Documentum CM Server to recreate the views.

1. Shut down the repository.
2. Connect to the database used by the repository through a SQL Editor. Connect as the repository owner.
3. Update the **views_valid** attribute for each corrupted object type using the following command:

   ```
   SQL> UPDATE dm_type_s SET views_valid = 0 WHERE name ='dm_document';
   ```

4. If you are not sure which views to rebuild, you can rebuild the views for all the existing object types using the following command:

   ```
   SQL> UPDATE dm_type_s SET views_valid = 0;
   ```

5. Commit the changes in the database.
6. Restart the repository.

After the views are recreated, the `views_valid` attribute will be automatically set to true (1).

4.6.7 Removing log4j 1.x files

You must remove the log4j 1.x files (`log4j.jar` and `log4j.properties`) from the following locations:

- Windows: `%Documentum%\Shared\log4j.jar` and `%Documentum%\config\log4j.properties`
- Linux: `$Documentum/dfc/log4j.jar` and `$Documentum/config/log4j.properties`

Chapter 5

Upgrading scenarios

This chapter describes some of the supported scenarios for upgrading a previous version of Documentum CM Server to 25.4. Each scenario describes the upgrade path for the Documentum CM Server including the base and upgraded versions of the operating system, database, and Documentum CM Server, and the steps you need to perform for the upgrade.

Notes

- Although there can be multiple upgrade scenarios depending on the operating system/database combination, it is not possible to document all of those scenarios.

  However, for a particular operating system/database combination, the upgrade steps do not vary much across Documentum CM Server versions. For example, if you are upgrading Documentum CM Server 16.7 on the Linux/Oracle environment, use the upgrade steps documented in the scenario, "Upgrading Documentum CM Server 20.4 to 25.4 – Linux/Oracle" on page 107.

- Upgrade from HashiCorp Vault-enabled environment to non-HashiCorp Vault environment is not supported.

5.1 Upgrading from 6.7 SP2 or 7.0 or 7.1 or 7.2 or 7.3 to 25.4

For any particular operating system/database combination, the upgrade steps do not vary much across Documentum CM Server versions 6.7 SP2, 7.0, 7.1, 7.2, and 7.3.

If your current installation is 6.7 SP2 or 7.0 or 7.1 or 7.2 or 7.3 and planning to upgrade to 25.4, you must perform the upgrade in the following sequence:

1. Upgrade from 6.7 SP2 or 7.0 or 7.1 or 7.2 or 7.3 to 16.4. After upgrading to 16.4, apply the 16.4 patch version, 42.
2. Upgrade from 16.4 Patch 42 to 25.4. You can use the information and instructions documented in the *OpenText Documentum System 22.4 Upgrade and Migration Guide* as a guidance.

5.2 Upgrading Documentum CM Server 16.4 to 25.4 – Windows/SQL Server

The following table lists the base and upgraded versions of the Documentum CM Server, operating system, and database that are supported in this upgrade scenario:

Table 5-1: Base and upgraded OS/DB/Documentum CM Server versions

	Base version	Upgraded version
Operating System	Windows Server 2016 (64-bit)	Windows Server 2022 (64-bit)
Database	SQL Server 2016	SQL Server 2022
Documentum CM Server	64-bit Documentum CM Server 16.4	64-bit Documentum CM Server 25.4

5.2.1 Pre-upgrade tasks

1. Review the "Upgrading Documentum CM Server" on page 35.
2. Back up the repository.
3. Ensure that you apply the latest Documentum CM Server patch.
4. Optional Take a backup of all users that are part of the *Admin group*. In addition, ensure that you take the backup of the customized attribute like group_address.
5. If the repository contains customized repository formats (dm_format objects), back up the customized formats.
6. Temporarily increase the amount of rollback space available in the RDBMS. The number of rollback segments should be commensurate with the size of the repository and should be in segments of equal size. For the steps, refer to the database documentation.
7. Ensure that you have sufficient disk space on the computer hosting the database.
8. Run the Consistency Checker tool. The syntax is:

```
dmbasic -fconsistency_checker.ebs -eEntry_Point -- <repository_name>
<superuser> <password>
```

9. Fix the inconsistencies reported by the Consistency Checker tool as errors.
10. Ensure that the dm_server_config object is unlocked.
11. Optional If you are upgrading Documentum CM Server enabled with SSL communication and lockbox, perform the following tasks:
    a. Remove the key from the lockbox using the following example command format:

```
dm_crypto_create -lockbox lockbox.lb -lockboxpassphrase Password@123 -keyname
CSaek -removelockbox -output CSaek
```

b. Comment the `crypto_lockbox` section from all the `docbroker.ini` and `server.ini` files.

c. Restart the connection broker and the repository and ensure that they start properly.

12. If you want to upgrade AEK key, make sure that you update the AEK passphrase to comply with password complexity rules using the following command format:

```
dm_crypto_change_passphrase.exe -keyname <name of aek key> -passphrase <old
passsphrase> -newpassphrase <new password with complexity rules>
```

For example:

```
dm_crypto_change_passphrase.exe -keyname aek_name -passphrase Password@123 -
newpassphrase Password@1234567890
```

The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about password complexity rules.

Note: This step is valid only when upgrading to a repository where HashiCorp Vault is not enabled.

13. If you want to upgrade AEK key in a repository where HashiCorp Vault is enabled, then you must create HashiCorp Vault-based AEK keys.

OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD) contains detailed information.

5.2.2 Upgrade tasks

1. Upgrade the Windows operating system to Windows Server 2022 (64-bit).
2. Install the latest version of Microsoft Visual C++ 2013, 2019, and 2022 Redistributable (64-bit) package before upgrading a repository. This provides the correct operating system runtime libraries for the Documentum CM Server and other utilities.
3. Upgrade the database to SQL Server 2022 for Microsoft Windows with latest cumulative update.
4. Disable all jobs.
   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
   b. Right-click the job and select **Properties**.
   c. On the **Properties** page, set the **State** to `Inactive`.
5. Shut down the repositories and connection brokers.
   a. Click **Start > Programs > Documentum > Server Manager**.

b. Select the correct Documentum CM Server and click **Stop**.

c. On the **Connection Broker** tab, select each connection broker, and then click **Stop**.

6. To shut down the application server on Windows, stop the service called `Java Method Server`. Ensure that the application server does not start automatically after a host restart.

   Click **Start > Control Panel > Administrative Tools > Services**, select the **Java Method Server**, and then click **Stop**.

7. Download and install the supported version of Oracle JDK/OpenJDK version from Oracle JDK/OpenJDK website. The *Oracle JDK and OpenJDK* documentation contains detailed information. "Using SSL communication" on page 34 provides more details about SSL communication with JDK.

8. Run the Documentum CM Server installation program.

   a. Run `serverSetup.exe`.

   b. Click **Yes** when the installer displays a message stating that you are trying to upgrade the older version and asks if you want to proceed.

   c. Accept the license agreement and click **Next**.

   d. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

   e. If you select the **Enable Vault** check box, provide the following information and click **Next**:

      i. **DSIS URL**: Provide a value in the following format:

      ```
      http://localhost:<port mentioned in application.properties>/dsis
      ```

      ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

      Important

      If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

   f. On Windows, provide the installation owner password and click **Next**.

      - If HashiCorp Vault is enabled, the installation owner password is retrieved from the HashiCorp Vault server.
      - If HashiCorp Vault is not enabled, type the installation owner password.

   g. Browse and specify the directory where the supported version of JDK is installed. Click **Next**.

   h. Set the administrator password and specify an available listening port for the embedded application server used by Documentum CM Server and click **Next**.

- **Admin User Password**: Application server password. You must follow the password complexity rules. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about the password complexity rules.
  - If HashiCorp Vault is enabled, then the application server password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, then type the application server password.
- **Listen Port**: The port on which the application server listens for standard administration connections. A total of 20 ports, starting from the one you specify is used by the application server, and all of them must be available. The default port number is 9080. Irrespective of you accepting the default port or choosing another one, do not change this port after the initial configuration.

i. Review the installation summary and click **Install** to begin installation.

j. To open the Documentum CM Server configuration program and configure the repository, select **Configure now** and click **Done**.

9. Upgrade the connection broker.

a. Open the Documentum CM Server configuration program.

b. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

c. If you select the **Enable Vault** check box, provide the following information and click **Next**:

i. **DSIS URL**: Provide a value in the following format:

```
http://localhost:<port mentioned in application.properties>/dsis
```

ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

> **Important**
> If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

d. Select **Connection broker** and click **Next**.

e. On Windows, provide the installation owner password and click **Next**.

- If HashiCorp Vault is enabled, the installation owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the installation owner password.

f. Select **Upgrade a connection broker**.

g. Select the connection broker to upgrade from the list and click **Next**.

h. Complete the configuration, select **Perform additional configuration**, and click **Next**.

10. Upgrade the existing repository.

a. On the configuration program options page, select **Repository**, and click **Next**.

b. Select **Upgrade an existing repository**.

c. Select the repository to upgrade from the list and click **Next**.

d. Documentum CM Server 16.7 and later versions do not support lockbox. For more information about creating new AEK key or use existing AEK key, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

e. Type the information for **Connection Broker Port** and **Connection Broker Host** and click **Next**.

f. Select the **Connection Mode** for the repository and click **Next**. If you select the **Secure** or **Native and Secure** options, select **Use certificate** on the next page and provide the required details.

If HashiCorp Vault is enabled, to prepare the certificate passwords, the contents of the `broker.pwd` and `server.pwd` files must be updated with the `<secret_name>/<key_name>`. For example:

In the `broker.pwd` file:

```
DOCBROKER_CERT_PASSWORD/<host name of connection broker>
```

In the `server.pwd` file:

```
DOCBASE_CERT_PASSWORD/<repository name>
```

Click **Next**.

g. Select the type of mail server, perform the tasks depending on the mail server you select, and click **Next**. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.

h. Optional Select **Enable External User Metrics Service** if you want to track external user transactions and click **Next**.

i. Optional Select the **XML Store** check box if you want XML Store, specify the following information, and click **Next**:

- **XML Store Host**: Host name of the machine where BaseX server is installed and running.
- **XML Store Port**: Port on which BaseX server is running.
- **XML Store Administrator/Superuser password**: Password of the admin user in BaseX.
  - If HashiCorp Vault is enabled, the XML Store administrator/ superuser password is retrieved from the HashiCorp Vault server.

- If HashiCorp Vault is not enabled, type the XML Store administrator/superuser password.

j. Specify the data file path for BaseX and click **Next**.

k. Provide the repository owner password and click **Next**.

- If HashiCorp Vault is enabled, the repository owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the repository owner password.

l. Select **Finish configuration** and click **Next**.

11. If you upgraded from an installation using FAST full-text indexing, and selected xPlore full-text indexing, you must restart Documentum CM Server again after you complete the Documentum CM Server configuration.

12. After you complete the Documentum CM Server configuration, create a nonunique index on the `dm_sysobject.r_object_id` and `r_aspect_name` properties by using the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dm_sysobject',
attribute='r_aspect_name',use_id_col=true
```

The inclusion of the use_id_col argument set to true automatically causes Documentum CM Server to include the r_object_id column in the index.

13. If you are upgrading a repository in a distributed environment that uses a Branch Office Caching Services and asynchronous write jobs, create an index on the `dmr_content_s` (`i_parked_state`, `r_object_id`) properties. Use the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dmr_content',
attribute='i_parked_state',use_id_col=true,id_in_front=false
```

5.2.3 Post-upgrade tasks

1. Complete the tasks as described in "Licensing OpenText Documentum CM" on page 59.

2. Enable all the disabled jobs.

   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.

   b. For each of the previously disabled jobs, right-click the job and select **Properties**.

   c. On the **Properties** page, set the **State** option to `Active`.

3. On a Windows upgrade, the **Startup Type** is set to **Manual** for the Documentum Docbase Service *repository name* service. If you want the repository to automatically start after a server reboot, navigate to **Start > All Programs > Administrative Tools > Services**, and set the **Startup Type** to **Automatic**.

4. Optional Run `dm_filestore_unique.class` in `%DM_HOME%\install\tools` to create a filestore lock file after upgrade. Processing result (success or failure) can be found in the log file.

5. After upgrade, ensure that you add the backed up list of users to the Admin group. In addition, ensure that you manually update the backed up customized attribute. Admin group is recreated as part of the upgrade process, which dissolves all group memberships for `admingroup`. Before the upgrade process, the administrator must document the groups which contain `admingroup` as a member. Similarly, the administrator must document any changes made to the `admingroup` itself. Recreation of memberships must be reapplied after completing the upgrade process.

6. After the upgrade is complete, perform the following verifications:

   a. Check whether the `<Docbroker>.log` file in the `<Documentum_Home>\dba\log\` folder contains any warning messages related to DM_DOCBROKER_W_SSL_HANDSHAKE_FAILED.

   b. Check whether the `<Docbase>.log` file in the `<Documentum_Home>\dba\log\` folder contain any exceptions or errors.

   c. Check for error messages in the `%DM_JMS_HOME%\logs\catalina<timestamp>.log` file.

   d. To check the OpenText Documentum CM version, in the command prompt, run the following command:

   ```
   documentum -version
   ```

   e. To check the Foundation Java API version, ensure that the JRE bin path is set in the `PATH` variable, and then in the command prompt, run the following command:

   ```
   java DfShowVersion
   ```

   f. You can also check the OpenText Documentum CM version mentioned in the repository and connection broker log files.

7. Enable the FIPS settings as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

8. Review "Post-upgrade tasks" on page 59 for other post-upgrade tasks that you might need to perform.

5.3 Upgrading Documentum CM Server 16.7 to 25.4 – Windows/Oracle

The following table lists the base and upgraded versions of the Documentum CM Server, operating system, and database that are supported in this upgrade scenario:

Table 5-2: Base and upgraded OS/DB/Documentum CM Server versions

	Base version	Upgraded version
Operating System	Windows Server 2016 (64-bit)	Windows Server 2022 (64-bit)
Database	Oracle 18.3	Oracle 19c
Documentum CM Server	64-bit Documentum CM Server 16.7	64-bit Documentum CM Server 25.4

5.3.1 Pre-upgrade tasks

Note: To make the upgrade process work faster, if you use functional or bitmap Oracle customized indexes in Oracle database, then drop them prior to the upgrade and recreate them after the migration.

1. Review the "Upgrading Documentum CM Server" on page 35.
2. If you are installing the xPlore indexing server, review the *OpenText Documentum xPlore Installation Guide*.
3. Back up the repository.
4. Optional Take a backup of all users that are part of the *Admin group*. In addition, ensure that you take the backup of the customized attribute like group_address.
5. If the repository contains customized repository formats (dm_format objects), back up the customized formats.
6. Temporarily increase the amount of rollback space available in the RDBMS. The number of rollback segments should be commensurate with the size of the repository and should be in segments of equal size. For the steps, refer to the database documentation.
7. Ensure that you have sufficient disk space on the computer hosting the database.
8. Run the Consistency Checker tool. The syntax is:

```
dmbasic -fconsistency_checker.ebs -eEntry_Point -- <repository_name>
<superuser> <password>
```

9. Fix the inconsistencies reported by the Consistency Checker tool as errors.
10. Ensure that the dm_server_config object is unlocked.

11. If you want to upgrade AEK key, make sure that you update the AEK passphrase to comply with password complexity rules using the following command format:

```
dm_crypto_change_passphrase.exe -keyname <name of aek key> -passphrase <old
passsphrase> -newpassphrase <new password with complexity rules>
```

For example:

```
dm_crypto_change_passphrase.exe -keyname aek_name -passphrase Password@123 -
newpassphrase Password@1234567890
```

The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about password complexity rules.

Note: This step is valid only when upgrading to a repository where HashiCorp Vault is not enabled.

12. If you want to upgrade AEK key in a repository where HashiCorp Vault is enabled, then you must create HashiCorp Vault-based AEK keys.

OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD) contains detailed information.

5.3.2 Upgrade tasks

1. Upgrade the Windows operating system to Windows Server 2022 (64-bit).
2. Install the latest version of Microsoft Visual C++ 2013, 2019, and 2022 Redistributable (64-bit) package before upgrading a repository. This provides the correct operating system runtime libraries for the Documentum CM Server and other utilities.
3. Upgrade the database to Oracle 19c.
4. After you upgrade the database, create an `ORACLE_HOME` environment variable in Windows that points to the location of the 64-bit `tnsnames.ora` file. The entries from the 32-bit `tnsnames.ora` file have to be copied into the 64-bit `tnsnames.ora` file.
5. Disable all jobs.
   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
   b. Right-click the job and select **Properties**.
   c. On the **Properties** page, set the **State** to `Inactive`.
6. Shut down the repositories and connection brokers.
   a. Click **Start > Programs > Documentum > Server Manager**.
   b. Select the correct Documentum CM Server and click **Stop**.
   c. On the **Connection Broker** tab, select each connection broker, and then click **Stop**.

7. To shut down the application server on Windows, stop the service called Java Method Server. Ensure that the application server does not start automatically after a host restart.

   Click **Start > Control Panel > Administrative Tools > Services**, select the **Java Method Server**, and then click **Stop**.

8. During the upgrade from 32-bit to 64-bit, Documentum CM Server, you cannot upgrade the authentication plug-ins that you have installed. You need to replace the 32-bit authentication plug-ins with the 64-bit plug-ins. You can find the plug-ins in the `%DM_HOME%\install\external_apps\authplugins` folder.

9. Download and install the supported version of Oracle JDK/OpenJDK version from Oracle JDK/OpenJDK website. The *Oracle JDK and OpenJDK* documentation contains detailed information. "Using SSL communication" on page 34 provides more details about SSL communication with JDK.

10. Run the Documentum CM Server installation program.

    a. Run `serverSetup.exe`.
    b. Click **Yes** when the installer displays a message stating that you are trying to upgrade the older version and asks if you want to proceed.
    c. Accept the license agreement and click **Next**.
    d. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.
    e. If you select the **Enable Vault** check box, provide the following information and click **Next**:

       i. **DSIS URL**: Provide a value in the following format:

       ```
       http://localhost:<port mentioned in application.properties>/dsis
       ```

       ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

       Important

       If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

    f. On Windows, provide the installation owner password and click **Next**.

       - If HashiCorp Vault is enabled, the installation owner password is retrieved from the HashiCorp Vault server.
       - If HashiCorp Vault is not enabled, type the installation owner password.

    g. Browse and specify the directory where the supported version of JDK is installed. Click **Next**.
    h. Set the administrator password and specify an available listening port for the embedded application server used by Documentum CM Server and click **Next**.

- **Admin User Password**: Application server password. You must follow the password complexity rules. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about the password complexity rules.
  - If HashiCorp Vault is enabled, then the application server password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, then type the application server password.
- **Listen Port**: The port on which the application server listens for standard administration connections. A total of 20 ports, starting from the one you specify is used by the application server, and all of them must be available. The default port number is 9080. Irrespective of you accepting the default port or choosing another one, do not change this port after the initial configuration.

i. Review the installation summary and click **Install** to begin installation.

j. To open the Documentum CM Server configuration program and configure the repository, select **Configure now** and click **Done**.

11. Upgrade the connection broker.

a. Open the Documentum CM Server configuration program.

b. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

c. If you select the **Enable Vault** check box, provide the following information and click **Next**:

i. **DSIS URL**: Provide a value in the following format:

```
http://localhost:<port mentioned in application.properties>/dsis
```

ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

> **Important**
> If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

d. Select **Connection broker** and click **Next**.

e. On Windows, provide the installation owner password and click **Next**.

- If HashiCorp Vault is enabled, the installation owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the installation owner password.

f. Select **Upgrade a connection broker**.

g. Select the connection broker to upgrade from the list and click **Next**.

h. Complete the configuration, select **Perform additional configuration**, and click **Next**.

12. Upgrade the existing repository.

a. On the configuration program options page, select **Repository** and then click **Next**.

b. Select **Upgrade an existing repository**.

c. Select the repository to upgrade from the list and click **Next**.

d. You can choose if you want to upgrade AEK key or continue with the existing AEK key. Take a backup of the AEK key. For creating new AEK key, refer to the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

e. Type the information for **Connection Broker Port** and **Connection Broker Host** and click **Next**.

f. Select the **Connection Mode** for the repository and click **Next**. If you select the **Secure** or **Native and Secure** options, select **Use certificate** on the next page and provide the required details.

If HashiCorp Vault is enabled, to prepare the certificate passwords, the contents of the `broker.pwd` and `server.pwd` files must be updated with the `<secret_name>/<key_name>`. For example:

In the `broker.pwd` file:

```
DOCBROKER_CERT_PASSWORD/<host name of connection broker>
```

In the `server.pwd` file:

```
DOCBASE_CERT_PASSWORD/<repository name>
```

Click **Next**.

g. Select the type of mail server, perform the tasks depending on the mail server you select, and click **Next**. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.

h. Optional Select **Enable External User Metrics Service** if you want to track external user transactions and click **Next**.

i. Optional Select the **XML Store** check box if you want XML Store, specify the following information, and click **Next**:

- **XML Store Host**: Host name of the machine where BaseX server is installed and running.
- **XML Store Port**: Port on which BaseX server is running.
- **XML Store Administrator/Superuser password**: Password of the admin user in BaseX.
  - If HashiCorp Vault is enabled, the XML Store administrator/ superuser password is retrieved from the HashiCorp Vault server.

– If HashiCorp Vault is not enabled, type the XML Store administrator/superuser password.

j. Specify the data file path for BaseX and click **Next**.

k. Provide the repository owner password and click **Next**.

- If HashiCorp Vault is enabled, the repository owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the repository owner password.

l. Select **Finish configuration** and click **Next**.

13. If you upgraded from an installation using FAST full-text indexing, and selected xPlore full-text indexing, you must restart Documentum CM Server again after you complete the Documentum CM Server configuration.

14. After you complete the Documentum CM Server configuration, create a nonunique index on the `dm_sysobject.r_object_id` and `r_aspect_name` properties by using the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dm_sysobject',
attribute='r_aspect_name',use_id_col=true
```

The inclusion of the use_id_col argument set to true automatically causes Documentum CM Server to include the r_object_id column in the index.

15. If you are upgrading a repository in a distributed environment that uses a Branch Office Caching Services and asynchronous write jobs, create an index on the `dmr_content_s` (`i_parked_state`, `r_object_id`) properties. Use the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dmr_content',
attribute='i_parked_state',use_id_col=true,id_in_front=false
```

5.3.3 Post-upgrade tasks

Follow the steps provided in "Post-upgrade tasks" on page 81.

5.4 Upgrading Documentum CM Server 16.7.1 to 25.4 – Linux/Oracle

The following table lists the base and upgraded versions of the Documentum CM Server, operating system, and database that are supported in this upgrade scenario:

Table 5-3: Base and upgraded OS/DB/Documentum CM Server versions

	Base version	Upgraded version
Operating System	Red Hat Enterprise Linux 7.7 (64-bit)	Red Hat Enterprise Linux 8.10 (64-bit)
Database	Oracle 18.3	Oracle 19c

	Base version	Upgraded version
Documentum CM Server	64-bit Documentum CM Server 16.7.1	64-bit Documentum CM Server 25.4

5.4.1 Pre-upgrade tasks

1. Review the "Upgrading Documentum CM Server" on page 35.
2. Back up the repository.
3. Optional Take a backup of all users that are part of the *Admin group*. In addition, ensure that you take the backup of the customized attribute like group_address.
4. If the repository contains customized repository formats (dm_format objects), back up the customized formats.
5. Temporarily increase the amount of rollback space available in the RDBMS. The number of rollback segments should be commensurate with the size of the repository and should be in segments of equal size. For the steps, refer to the database documentation.
6. Ensure that you have sufficient disk space on the computer hosting the database.
7. Run the Consistency Checker tool. The syntax is:

   ```
   dmbasic -fconsistency_checker.ebs -eEntry_Point -- <repository_name>
   <superuser> <password>
   ```

8. Fix the inconsistencies reported by the Consistency Checker tool as errors.
9. Ensure that the dm_server_config object is unlocked.
10. Ensure that you perform the tasks mentioned in step step 17 in "Upgrade checklist" on page 35.
11. If you want to upgrade AEK key, make sure that you update the AEK passphrase to comply with password complexity rules using the following command format:

    ```
    dm_crypto_change_passphrase.exe -keyname <name of aek key> -passphrase <old
    passsphrase> -newpassphrase <new password with complexity rules>
    ```

    For example:

    ```
    dm_crypto_change_passphrase.exe -keyname aek_name -passphrase Password@123 -
    newpassphrase Password@1234567890
    ```

    The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about password complexity rules.

    Note: This step is valid only when upgrading to a repository where HashiCorp Vault is not enabled.

12. If you want to upgrade AEK key in a repository where HashiCorp Vault is enabled, then you must create HashiCorp Vault-based AEK keys.

    OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD) contains detailed information.

5.4.2 Upgrade tasks

1. Upgrade the Linux operating system to Red Hat Enterprise Linux 8.10 (64-bit).
2. Upgrade the database to Oracle 19c.
3. Disable all jobs.
   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
   b. Right-click the job and select **Properties**.
   c. On the **Properties** page, set the **State** to `Inactive`.
4. Shut down the repositories and connection brokers.
   a. For each repository, run the `dm_shutdown_repository` script, where repository is the name of the Documentum CM Server to be stopped.
   b. Stop each connection broker using the `dm_stop_docbroker` utility on the command line:

   ```
   % dm_stop_docbroker [-Ppassword][-B[batch]] [-Nport_number][-Sservice_name]
   ```

5. To shut down the application server on Linux, stop the service called Java Method Server. Ensure that the application server does not start automatically after a host restart.

   Run the script `$DM_JMS_HOME/bin/stopMethodServer.sh`.

6. Download and install the supported version of Oracle JDK/OpenJDK version from Oracle JDK/OpenJDK website. The *Oracle JDK and OpenJDK* documentation contains detailed information. "Using SSL communication" on page 34 provides more information.
7. Run the random generator as root using the following command:

   ```
   /sbin/rngd -b -r /dev/urandom -o /dev/random
   ```

   Note: If the operating system is upgraded to Linux 7.x/8.x/9.x, then run the following command as root:

   ```
   ln -s /usr/lib64/libsasl2.so.3.0.0 /usr/lib64/libsasl2.so.2
   ```

8. Run the Documentum CM Server installation program.
   a. Run `serverSetup.bin`.

   Note: Before you install Documentum CM Server on Linux, ensure that you have completed the following tasks:

- Install the Expect version 5.45.4 or earlier script utility.
- Install the TCL version 8.6.8 or earlier script utility.

The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more details.

b. Click **Yes** when the installer displays a message stating that you are trying to upgrade the older version and asks if you want to proceed.

c. Accept the license agreement and click **Next**.

d. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

e. If you select the **Enable Vault** check box, provide the following information and click **Next**:

i. **DSIS URL**: Provide a value in the following format:

```
http://localhost:<port mentioned in application.properties>/dsis
```

ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

> **Important**
> If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

f. Browse and specify the directory where the supported version of JDK is installed. Click **Next**.

g. Set the administrator password and specify an available listening port for the embedded application server used by Documentum CM Server and click **Next**.

- **Admin User Password**: Application server password. You must follow the password complexity rules. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about the password complexity rules.
  - If HashiCorp Vault is enabled, then the application server password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, then type the application server password.
- **Listen Port**: The port on which the application server listens for standard administration connections. A total of 20 ports, starting from the one you specify is used by the application server, and all of them must be available. The default port number is 9080. Irrespective of you accepting the default port or choosing another one, do not change this port after the initial configuration.

h. Review the installation summary and click **Install** to begin installation.

i. To open the Documentum CM Server configuration program and configure the repository, select **Configure now** and click **Done**.

9. Upgrade the connection broker.

a. Open the Documentum CM Server configuration program.

b. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

c. If you select the **Enable Vault** check box, provide the following information and click **Next**:

i. **DSIS URL**: Provide a value in the following format:

```
http://localhost:<port mentioned in application.properties>/dsis
```

ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

> **Important**
> If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

d. Select **Connection broker** and click **Next**.

e. Select **Upgrade a connection broker**.

f. Select the connection broker to upgrade from the list and click **Next**.

g. Complete the configuration, select **Perform additional configuration**, and click **Next**.

10. Upgrade the existing repository.

a. On the configuration program options page, select **Repository** and click **Next**.

b. Select **Upgrade an existing repository**.

c. Select the repository to upgrade from the list and click **Next**.

d. You can choose if you want to upgrade AEK key or continue with the existing AEK key. Take a backup of the AEK key. For creating new AEK key, refer to the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

e. Type the information for **Connection Broker Port** and **Connection Broker Host** and click **Next**.

f. Select the **Connection Mode** for the repository and click **Next**. If you select the **Secure** or **Native and Secure** options, select **Use certificate** on the next page and provide the required details.

If HashiCorp Vault is enabled, to prepare the certificate passwords, the contents of the `broker.pwd` and `server.pwd` files must be updated with the `<secret_name>/<key_name>`. For example:

In the `broker.pwd` file:

```
DOCBROKER_CERT_PASSWORD/<host name of connection broker>
```

In the `server.pwd` file:

```
DOCBASE_CERT_PASSWORD/<repository name>
```

Click **Next**.

g. Select the type of mail server, perform the tasks depending on the mail server you select, and click **Next**. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.

h. Optional Select **Enable External User Metrics Service** if you want to track the external user transactions and click **Next**.

i. Optional Select the **XML Store** check box if you want XML Store, specify the following information, and click **Next**:

- **XML Store Host**: Host name of the machine where BaseX server is installed and running.
- **XML Store Port**: Port on which BaseX server is running.
- **XML Store Administrator/Superuser password**: Password of the admin user in BaseX.
  - If HashiCorp Vault is enabled, the XML Store administrator/superuser password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, type the XML Store administrator/superuser password.

j. Specify the data file path for BaseX and click **Next**.

k. Provide the repository owner password and click **Next**.

- If HashiCorp Vault is enabled, the repository owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the repository owner password.

l. Select **Finish configuration** and click **Next**.

11. If you upgraded from an installation using FAST full-text indexing, and selected xPlore full-text indexing, you must restart Documentum CM Server again after you complete the Documentum CM Server configuration.

12. After you complete the Documentum CM Server configuration, create a nonunique index on the `dm_sysobject.r_object_id` and `r_aspect_name` properties by using the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dm_sysobject',
attribute='r_aspect_name',use_id_col=true
```

The inclusion of the use_id_col argument set to true automatically causes Documentum CM Server to include the r_object_id column in the index.

13. If you are upgrading a repository in a distributed environment that uses a Branch Office Caching Services and asynchronous write jobs, create an index on the dmr_content_s (i_parked_state, r_object_id) properties. Use the following MAKE_INDEX command:

```
EXECUTE make_index WITH type_name='dmr_content',
attribute='i_parked_state',use_id_col=true,id_in_front=false
```

5.4.3 Post-upgrade tasks

1. Complete the tasks as described in "Licensing OpenText Documentum CM" on page 59.
2. Manually run the dm_root_task as root.
3. Enable all the disabled jobs.
   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
   b. For each of the previously disabled jobs, right-click the job and select **Properties**.
   c. On the **Properties** page, set the **State** option to Active.
4. Optional Run dm_filestore_unique.class in $DM_HOME/install/tools to create a filestore lock file after upgrade. Processing result (success or failure) can be found in the log file.
5. After upgrade, ensure that you add the backed up list of users to the Admin group. In addition, ensure that you manually update the backed up customized attribute. Admin group is recreated as part of the upgrade process, which dissolves all group memberships for admingroup. Before the upgrade process, the administrator must document the groups which contain admingroup as a member. Similarly, the administrator must document any changes made to the admingroup itself. Recreation of memberships must be reapplied after completing the upgrade process.
6. After the upgrade is complete, perform the following verifications:
   a. Check whether the <Docbroker>.log file in the <Documentum_Home>/dba/log/ folder contains any warning messages related to DM_DOCBROKER_W_SSL_HANDSHAKE_FAILED.
   b. Check whether the <Docbase>.log file in the <Documentum_Home>/dba/log/ folder contain any exceptions or errors.
   c. Check for error messages in the $DM_JMS_HOME/logs/catalina<timestamp>.log file.
   d. To check the OpenText Documentum CM version, in the command prompt, run the following command:

```
documentum -version
```

   e. To check the Foundation Java API version, ensure that the JRE bin path is set in the *<PATH>* variable, and then in the command prompt, run the following command:

```
java DfShowVersion
```

f. You can also check the OpenText Documentum CM version mentioned in the repository and connection broker log files.

7. Enable the FIPS settings as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

8. Review "Post-upgrade tasks" on page 59 for other post-upgrade tasks that you might need to perform.

5.5 Upgrading Documentum CM Server 20.2 to 25.4 – Windows/PostgreSQL

The following table lists the base and upgraded versions of the Documentum CM Server, operating system, and database that are supported in this upgrade scenario:

Table 5-4: Base and upgraded OS/DB/Documentum CM Server versions

	Base version	Upgraded version
Operating System	Windows Server 2019 (64-bit)	Windows Server 2022 (64-bit)
Database	PostgreSQL 11	PostgreSQL 16.x
Documentum CM Server	64-bit Documentum CM Server 20.2	64-bit Documentum CM Server 25.4

5.5.1 Pre-upgrade tasks

1. Review the "Upgrading Documentum CM Server" on page 35.

2. If you are installing the xPlore indexing server, review the *OpenText Documentum xPlore Installation Guide*.

3. Back up the repository.

4. Optional Take a backup of all users that are part of the *Admin group*. In addition, ensure that you take the backup of the customized attribute like group_address.

5. If the repository contains customized repository formats (dm_format objects), back up the customized formats.

6. Ensure that you have sufficient disk space on the computer hosting the database.

7. Run the Consistency Checker tool. The syntax is:

```
dmbasic -fconsistency_checker.ebs -eEntry_Point -- <repository_name>
<superuser> <password>
```

8. Fix the inconsistencies reported by the Consistency Checker tool as errors.

9. Ensure that the dm_server_config object is unlocked.

10. If you want to upgrade AEK key, make sure that you update the AEK passphrase to comply with password complexity rules using the following command format:

```
dm_crypto_change_passphrase.exe -keyname <name of aek key> -passphrase <old
passsphrase> -newpassphrase <new password with complexity rules>
```

For example:

```
dm_crypto_change_passphrase.exe -keyname aek_name -passphrase Password@123 -
newpassphrase Password@1234567890
```

The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about password complexity rules.

Note: This step is valid only when upgrading to a repository where HashiCorp Vault is not enabled.

11. If you want to upgrade AEK key in a repository where HashiCorp Vault is enabled, then you must create HashiCorp Vault-based AEK keys.

OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD) contains detailed information.

5.5.2 Upgrade tasks

1. Upgrade the Windows operating system to Windows Server 2022 (64-bit).
2. Upgrade the database to PostgreSQL 16.x.
3. Disable all jobs.
   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
   b. Right-click the job and select **Properties**.
   c. On the **Properties** page, set the **State** to `Inactive`.
4. Shut down the repositories and connection brokers.
   a. Click **Start > Programs > Documentum > Server Manager**.
   b. Select the correct Documentum CM Server and click **Stop**.
   c. On the **Connection Broker** tab, select each connection broker and click **Stop**.
5. To shut down the application server on Windows, stop the service called Java Method Server. Ensure that the application server does not start automatically after a host restart.

   Click **Start > Control Panel > Administrative Tools > Services**, select the **Java Method Server**, and click **Stop**.
6. Download and install the supported version of Oracle JDK/OpenJDK version from Oracle JDK/OpenJDK website. The *Oracle JDK and OpenJDK*

documentation contains detailed information. "Using SSL communication" on page 34 provides more details about SSL communication with JDK.

7. Run the Documentum CM Server installation program.

   a. Run `serverSetup.bin`.

      Note: Before you install Documentum CM Server on Linux, ensure that you have completed the following tasks:

      - Install the Expect version 5.45.4 or earlier script utility.
      - Install the TCL version 8.6.8 or earlier script utility.

      The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more details.

   b. Click **Yes** when the installer displays a message stating that you are trying to upgrade the older version and asks if you want to proceed.

   c. Accept the license agreement and click **Next**.

   d. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

   e. If you select the **Enable Vault** check box, provide the following information and click **Next**:

      i. **DSIS URL**: Provide a value in the following format:

      ```
      http://localhost:<port mentioned in application.properties>/dsis
      ```

      ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

      Important

      If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

   f. Browse and specify the directory where the supported version of JDK is installed. Click **Next**.

   g. Set the administrator password and specify an available listening port for the embedded application server used by Documentum CM Server and click **Next**.

      - **Admin User Password**: Application server password. You must follow the password complexity rules. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about the password complexity rules.

        – If HashiCorp Vault is enabled, then the application server password is retrieved from the HashiCorp Vault server.

  - If HashiCorp Vault is not enabled, then type the application server password.

- **Listen Port**: The port on which the application server listens for standard administration connections. A total of 20 ports, starting from the one you specify is used by the application server, and all of them must be available. The default port number is 9080. Irrespective of you accepting the default port or choosing another one, do not change this port after the initial configuration.

h. Review the installation summary and click **Install** to begin installation.

i. To open the Documentum CM Server configuration program and configure the repository, select **Configure now** and click **Done**.

8. Upgrade the connection broker.

   a. Open the Documentum CM Server configuration program.

   b. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

   c. If you select the **Enable Vault** check box, provide the following information and click **Next**:

      i. **DSIS URL**: Provide a value in the following format:

      ```
      http://localhost:<port mentioned in application.properties>/dsis
      ```

      ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

      Important

      If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

   d. Select **Connection broker** and click **Next**.

   e. Select **Upgrade a connection broker**.

   f. Select the connection broker to upgrade from the list and click **Next**.

   g. Complete the configuration, select **Perform additional configuration**, and click **Next**.

9. Upgrade the existing repository.

   a. On the configuration program options page, select **Repository** and then click **Next**.

   b. Select **Upgrade an existing repository**.

   c. Select the repository to upgrade from the list, and click **Next**.

   d. For creating new AEK key or use existing AEK key, refer to the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

e. Type the **Connection Broker Port** and **Connection Broker Host** and click **Next**.

f. Select the **Connection Mode** for the repository and click **Next**. If you select the **Secure** or **Native and Secure** options, select **Use certificate** on the next page and provide the required details.

If HashiCorp Vault is enabled, to prepare the certificate passwords, the contents of the `broker.pwd` and `server.pwd` files must be updated with the `<secret_name>/<key_name>`. For example:

In the `broker.pwd` file:

```
DOCBROKER_CERT_PASSWORD/<host name of connection broker>
```

In the `server.pwd` file:

```
DOCBASE_CERT_PASSWORD/<repository name>
```

Click **Next**.

g. Select the type of mail server, perform the tasks depending on the mail server you select, and click **Next**. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.

h. Optional Select **Enable External User Metrics Service** if you want to track the external user transactions and click **Next**.

i. Optional Select the **XML Store** check box if you want XML Store, specify the following information, and click **Next**:

- **XML Store Host**: Host name of the machine where BaseX server is installed and running.
- **XML Store Port**: Port on which BaseX server is running.
- **XML Store Administrator/Superuser password**: Password of the admin user in BaseX.
  - If HashiCorp Vault is enabled, the XML Store administrator/superuser password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, type the XML Store administrator/superuser password.

j. Specify the data file path for BaseX and click **Next**.

k. Provide the repository owner password and click **Next**.

- If HashiCorp Vault is enabled, the repository owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the repository owner password.

l. Select **Finish configuration** and click **Next**.

10. If you upgraded from an installation using FAST full-text indexing, and selected xPlore full-text indexing, you must restart Documentum CM Server again after you complete the Documentum CM Server configuration.

11. After you complete the Documentum CM Server configuration, create a nonunique index on the `dm_sysobject.r_object_id` and `r_aspect_name` properties by using the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dm_sysobject',
attribute='r_aspect_name',use_id_col=true
```

    The inclusion of the use_id_col argument set to true automatically causes Documentum CM Server to include the r_object_id column in the index.

12. If you are upgrading a repository in a distributed environment that uses a Branch Office Caching Services and asynchronous write jobs, create an index on the `dmr_content_s` (`i_parked_state`, `r_object_id`) properties. Use the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dmr_content',
attribute='i_parked_state',use_id_col=true,id_in_front=false
```

5.5.3 Post-upgrade tasks

Follow the steps provided in "Post-upgrade tasks" on page 81.

5.6 Upgrading Documentum CM Server 20.3 to 25.4 – Linux/PostgreSQL

The following table lists the base and upgraded versions of the Documentum CM Server, operating system, and database that are supported in this upgrade scenario:

Table 5-5: Base and upgraded OS/DB/Documentum CM Server versions

	Base version	Upgraded version
Operating System	Red Hat Enterprise Linux 7.x (64-bit)	Red Hat Enterprise Linux 9.x (64-bit)
Database	PostgreSQL 12	PostgreSQL 17.x
Documentum CM Server	64-bit Documentum CM Server 20.3	64-bit Documentum CM Server 25.4

5.6.1 Pre-upgrade tasks

1. Review the "Upgrading Documentum CM Server" on page 35.
2. Back up the repository.
3. Ensure that you apply the latest Documentum CM Server patch.
4. Optional Take a backup of all users that are part of the *Admin group*. In addition, ensure that you take the backup of the customized attribute like group_address.
5. If the repository contains customized repository formats (dm_format objects), back up the customized formats.

6. Run the Consistency Checker tool. The syntax is:

```
dmbasic -fconsistency_checker.ebs -eEntry_Point -- <repository_name>
<superuser> <password>
```

7. Fix the inconsistencies reported by the Consistency Checker tool as errors.
8. Ensure that the dm_server_config object is unlocked.
9. Ensure that you perform the tasks mentioned in step step 17 in "Upgrade checklist" on page 35.
10. If you want to upgrade AEK key, make sure that you update the AEK passphrase to comply with password complexity rules using the following command format:

```
dm_crypto_change_passphrase.exe -keyname <name of aek key> -passphrase <old
passsphrase> -newpassphrase <new password with complexity rules>
```

For example:

```
dm_crypto_change_passphrase.exe -keyname aek_name -passphrase Password@123 -
newpassphrase Password@1234567890
```

The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about password complexity rules.

Note: This step is valid only when upgrading to a repository where HashiCorp Vault is not enabled.

11. If you want to upgrade AEK key in a repository where HashiCorp Vault is enabled, then you must create HashiCorp Vault-based AEK keys.

OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD) contains detailed information.

5.6.2 Upgrade tasks

1. Upgrade the Linux operating system to Red Hat Enterprise Linux 8.x (64-bit).
2. Upgrade the Red Hat Enterprise Linux 8.x (64-bit) to Red Hat Enterprise Linux 9.x (64-bit).
3. Upgrade the database to PostgreSQL 17.x.
4. Disable all jobs.
   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
   b. Right-click the job and select **Properties**.
   c. On the **Properties** page, set the **State** to `Inactive`.
5. Shut down the repositories and connection brokers.
   a. For each repository, run the `dm_shutdown_repository` script, where repository is the name of the Documentum CM Server to be stopped.

b. Stop each connection broker using the `dm_stop_docbroker` utility on the command line:

```
% dm_stop_docbroker [-Ppassword][-B[batch]] [-Nport_number][-Sservice_name]
```

6. To shut down the application server on Linux, stop the service called Java Method Server. Ensure that the application server does not start automatically after a host restart.

   Run the script `$DM_JMS_HOME/bin/stopMethodServer.sh`.

7. Download and install the supported version of Oracle JDK/OpenJDK version from Oracle JDK/OpenJDK website. The *Oracle JDK and OpenJDK* documentation contains detailed information. "Using SSL communication" on page 34 provides more details about SSL communication with JDK.

8. Run the random generator as root using the following command:

```
/sbin/rngd -b -r /dev/urandom -o /dev/random
```

   Note: If the operating system is upgraded to Linux 7.x/8.x/9.x, then run the following command as root:

```
ln -s /usr/lib64/libsasl2.so.3.0.0 /usr/lib64/libsasl2.so.2
```

9. Run the Documentum CM Server installation program.

   a. Run `serverSetup.bin`.

      Note: Before you install Documentum CM Server on Linux, ensure that you have completed the following tasks:

      - Install the Expect version 5.45.4 or earlier script utility.
      - Install the TCL version 8.6.8 or earlier script utility.

      The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more details.

   b. Click **Yes** when the installer displays a message stating that you are trying to upgrade the older version and asks if you want to proceed.

   c. Accept the license agreement and click **Next**.

   d. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

   e. If you select the **Enable Vault** check box, provide the following information and click **Next**:

      i. **DSIS URL**: Provide a value in the following format:

```
http://localhost:<port mentioned in application.properties>/dsis
```

      ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

> **Important**
> If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

f. Browse and specify the directory where the supported version of JDK is installed. Click **Next**.

g. Set the administrator password and specify an available listening port for the embedded application server used by Documentum CM Server and click **Next**.

- **Admin User Password**: Application server password. You must follow the password complexity rules. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about the password complexity rules.
  - If HashiCorp Vault is enabled, then the application server password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, then type the application server password.
- **Listen Port**: The port on which the application server listens for standard administration connections. A total of 20 ports, starting from the one you specify is used by the application server, and all of them must be available. The default port number is 9080. Irrespective of you accepting the default port or choosing another one, do not change this port after the initial configuration.

h. Review the installation summary and click **Install** to begin installation.

i. To open the Documentum CM Server configuration program and configure the repository, select **Configure now** and click **Done**.

10. Upgrade the connection broker.

a. Open the Documentum CM Server configuration program.

b. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

c. If you select the **Enable Vault** check box, provide the following information and click **Next**:

i. **DSIS URL**: Provide a value in the following format:

```
http://localhost:<port mentioned in application.properties>/dsis
```

ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

> **Important**
> If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make

sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

d. Select **Connection broker** and click **Next**.

e. Select **Upgrade a connection broker**.

f. Select the connection broker to upgrade from the list and click **Next**.

g. Complete the configuration, select **Perform additional configuration**, and click **Next**.

11. Upgrade the existing repository.

a. On the configuration program options page, select **Repository** and then click **Next**.

b. Select **Upgrade an existing repository**.

c. Select the repository to upgrade from the list, and click **Next**.

d. For creating new AEK key or use existing AEK key, refer to the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

e. Type the **Connection Broker Port** and **Connection Broker Host** and click **Next**.

f. Select the **Connection Mode** for the repository and click **Next**. If you select the **Secure** or **Native and Secure** options, select **Use certificate** on the next page and provide the required details.

If HashiCorp Vault is enabled, to prepare the certificate passwords, the contents of the `broker.pwd` and `server.pwd` files must be updated with the `<secret_name>/<key_name>`. For example:

In the `broker.pwd` file:

```
DOCBROKER_CERT_PASSWORD/<host name of connection broker>
```

In the `server.pwd` file:

```
DOCBASE_CERT_PASSWORD/<repository name>
```

Click **Next**.

g. Select the type of mail server, perform the tasks depending on the mail server you select, and click **Next**. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.

h. Optional Select **Enable External User Metrics Service** if you want to track the external user transactions and click **Next**.

i. Optional Select the **XML Store** check box if you want XML Store, specify the following information, and click **Next**:

- **XML Store Host**: Host name of the machine where BaseX server is installed and running.
- **XML Store Port**: Port on which BaseX server is running.

- **XML Store Administrator/Superuser password**: Password of the admin user in BaseX.
  - If HashiCorp Vault is enabled, the XML Store administrator/ superuser password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, type the XML Store administrator/superuser password.

j. Specify the data file path for BaseX and click **Next**.

k. Provide the repository owner password and click **Next**.

- If HashiCorp Vault is enabled, the repository owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the repository owner password.

l. Select **Finish configuration** and click **Next**.

12. If you upgraded from an installation using FAST full-text indexing, and selected xPlore full-text indexing, you must restart Documentum CM Server again after you complete the Documentum CM Server configuration.

13. After you complete the Documentum CM Server configuration, create a nonunique index on the `dm_sysobject.r_object_id` and `r_aspect_name` properties by using the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dm_sysobject',
attribute='r_aspect_name',use_id_col=true
```

The inclusion of the use_id_col argument set to true automatically causes Documentum CM Server to include the r_object_id column in the index.

14. If you are upgrading a repository in a distributed environment that uses a Branch Office Caching Services and asynchronous write jobs, create an index on the `dmr_content_s` (`i_parked_state`, `r_object_id`) properties. Use the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dmr_content',
attribute='i_parked_state',use_id_col=true,id_in_front=false
```

5.6.3 Post-upgrade tasks

1. Complete the tasks as described in "Licensing OpenText Documentum CM" on page 59.

2. Manually run the `dm_root_task` as root.

3. Enable all the disabled jobs.

   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.

   b. For each of the previously disabled jobs, right-click the job and select **Properties**.

   c. On the **Properties** page, set the **State** option to `Active`.

4. Optional Run `dm_filestore_unique.class` in `$DM_HOME/install/tools` to create a filestore lock file after upgrade. Processing result (success or failure) can be found in the log file.

5. After upgrade, ensure that you add the backed up list of users to the Admin group. In addition, ensure that you manually update the backed up customized attribute. Admin group is recreated as part of the upgrade process, which dissolves all group memberships for `admingroup`. Before the upgrade process, the administrator must document the groups which contain `admingroup` as a member. Similarly, the administrator must document any changes made to the `admingroup` itself. Recreation of memberships must be reapplied after completing the upgrade process.

6. After the upgrade is complete, perform the following verifications:

   a. Check whether the `<Docbroker>.log` file in the `<Documentum_Home>/dba/log/` folder contains any warning messages related to DM_DOCBROKER_W_SSL_HANDSHAKE_FAILED.

   b. Check whether the `<Docbase>.log` file in the `<Documentum_Home>/dba/log/` folder contain any exceptions or errors.

   c. Check for error messages in the `$DM_JMS_HOME/logs/catalina<timestamp>.log` file.

   d. To check the OpenText Documentum CM version, in the command prompt, run the following command:

   ```
   documentum -version
   ```

   e. To check the Foundation Java API version, ensure that the JRE bin path is set in the <*PATH*> variable, and then in the command prompt, run the following command:

   ```
   java DfShowVersion
   ```

   f. You can also check the OpenText Documentum CM version mentioned in the repository and connection broker log files.

7. Enable the FIPS settings as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

8. Review "Post-upgrade tasks" on page 59 for other post-upgrade tasks that you might need to perform.

5.7 Upgrading Documentum CM Server 20.4 to 25.4 – Linux/Oracle

The following table lists the base and upgraded versions of the Documentum CM Server, operating system, and database that are supported in this upgrade scenario:

Table 5-6: Base and upgraded OS/DB/Documentum CM Server versions

	Base version	Upgraded version
Operating System	Red Hat Enterprise Linux 8.0 (64-bit)	Red Hat Enterprise Linux 8.10 (64-bit)
Database	Oracle 18.3	Oracle 19c
Documentum CM Server	64-bit Documentum CM Server 20.4	64-bit Documentum CM Server 25.4

5.7.1 Pre-upgrade tasks

1. Review the "Upgrading Documentum CM Server" on page 35.
2. Back up the repository.
3. Optional Take a backup of all users that are part of the *Admin group*. In addition, ensure that you take the backup of the customized attribute like group_address.
4. If the repository contains customized repository formats (dm_format objects), back up the customized formats.
5. Temporarily increase the amount of rollback space available in the RDBMS. The number of rollback segments should be commensurate with the size of the repository and should be in segments of equal size. For the steps, refer to the database documentation.
6. Ensure that you have sufficient disk space on the computer hosting the database.
7. Run the Consistency Checker tool. The syntax is:

```
dmbasic -fconsistency_checker.ebs -eEntry_Point -- <repository_name>
<superuser> <password>
```

8. Fix the inconsistencies reported by the Consistency Checker tool as errors.
9. Ensure that the dm_server_config object is unlocked.
10. Ensure that you perform the tasks mentioned in step step 17 in "Upgrade checklist" on page 35.
11. If you want to upgrade AEK key, make sure that you update the AEK passphrase to comply with password complexity rules using the following command format:

```
dm_crypto_change_passphrase.exe -keyname <name of aek key> -passphrase <old
passsphrase> -newpassphrase <new password with complexity rules>
```

For example:

```
dm_crypto_change_passphrase.exe -keyname aek_name -passphrase Password@123 -
newpassphrase Password@1234567890
```

The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about password complexity rules.

Note: This step is valid only when upgrading to a repository where HashiCorp Vault is not enabled.

12. If you want to upgrade AEK key in a repository where HashiCorp Vault is enabled, then you must create HashiCorp Vault-based AEK keys.

    OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD) contains detailed information.

5.7.2 Upgrade tasks

1. Upgrade the Linux operating system to Red Hat Enterprise Linux 8.10 (64-bit).
2. Upgrade the database to Oracle 19c.
3. Disable all jobs.
   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
   b. Right-click the job and select **Properties**.
   c. On the **Properties** page, set the **State** to `Inactive`.
4. Shut down the repositories and connection brokers.
   a. For each repository, run the `dm_shutdown_repository` script, where repository is the name of the Documentum CM Server to be stopped.
   b. Stop each connection broker using the `dm_stop_docbroker` utility on the command line:

      ```
      % dm_stop_docbroker [-Ppassword][-B[batch]] [-Nport_number][-Sservice_name]
      ```
5. To shut down the application server on Linux, stop the service called Java Method Server. Ensure that the application server does not start automatically after a host restart.

   Run the script `$DM_JMS_HOME/bin/stopMethodServer.sh`.
6. Download and install the supported version of Oracle JDK/OpenJDK version from Oracle JDK/OpenJDK website. The *Oracle JDK and OpenJDK* documentation contains detailed information. "Using SSL communication" on page 34 provides more information.
7. Run the random generator as root using the following command:

```
/sbin/rngd -b -r /dev/urandom -o /dev/random
```

Note: If the operating system is upgraded to Linux 7.x/8.x/9.x, then run the following command as root:

```
ln -s /usr/lib64/libsasl2.so.3.0.0 /usr/lib64/libsasl2.so.2
```

8. Run the Documentum CM Server installation program.

   a. Run `serverSetup.bin`.

      Note: Before you install Documentum CM Server on Linux, ensure that you have completed the following tasks:

      - Install the Expect version 5.45.4 or earlier script utility.
      - Install the TCL version 8.6.8 or earlier script utility.

      The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more details.

   b. Click **Yes** when the installer displays a message stating that you are trying to upgrade the older version and asks if you want to proceed.

   c. Accept the license agreement and click **Next**.

   d. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

   e. If you select the **Enable Vault** check box, provide the following information and click **Next**:

      i. **DSIS URL**: Provide a value in the following format:

      ```
      http://localhost:<port mentioned in application.properties>/dsis
      ```

      ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

      Important

      If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

   f. Browse and specify the directory where the supported version of JDK is installed. Click **Next**.

   g. Set the administrator password and specify an available listening port for the embedded application server used by Documentum CM Server and click **Next**.

      - **Admin User Password**: Application server password. You must follow the password complexity rules. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide*

(EDCSY250400-IGD) contains detailed information about the password complexity rules.

  - If HashiCorp Vault is enabled, then the application server password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, then type the application server password.

- **Listen Port**: The port on which the application server listens for standard administration connections. A total of 20 ports, starting from the one you specify is used by the application server, and all of them must be available. The default port number is 9080. Irrespective of you accepting the default port or choosing another one, do not change this port after the initial configuration.

h. Review the installation summary and click **Install** to begin installation.

i. To open the Documentum CM Server configuration program and configure the repository, select **Configure now** and click **Done**.

9. Upgrade the connection broker.

   a. Open the Documentum CM Server configuration program.

   b. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

   c. If you select the **Enable Vault** check box, provide the following information and click **Next**:

      i. **DSIS URL**: Provide a value in the following format:

      ```
      http://localhost:<port mentioned in application.properties>/dsis
      ```

      ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

      Important

      If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

   d. Select **Connection broker** and click **Next**.

   e. Select **Upgrade a connection broker**.

   f. Select the connection broker to upgrade from the list and click **Next**.

   g. Complete the configuration, select **Perform additional configuration**, and click **Next**.

10. Upgrade the existing repository.

    a. On the configuration program options page, select **Repository** and then click **Next**.

    b. Select **Upgrade an existing repository**.

c. Select the repository to upgrade from the list, and click **Next**.

d. You can choose if you want to upgrade AEK key or continue with the existing AEK key. Take a backup of the AEK key. For creating new AEK key, refer to the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

e. Type the **Connection Broker Port** and **Connection Broker Host** and click **Next**.

f. Select the **Connection Mode** for the repository and click **Next**. If you select the **Secure** or **Native and Secure** options, select **Use certificate** on the next page and provide the required details.

   If HashiCorp Vault is enabled, to prepare the certificate passwords, the contents of the `broker.pwd` and `server.pwd` files must be updated with the `<secret_name>/<key_name>`. For example:

   In the `broker.pwd` file:

   ```
   DOCBROKER_CERT_PASSWORD/<host name of connection broker>
   ```

   In the `server.pwd` file:

   ```
   DOCBASE_CERT_PASSWORD/<repository name>
   ```

   Click **Next**.

g. Select the type of mail server, perform the tasks depending on the mail server you select, and click **Next**. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.

h. Optional Select **Enable External User Metrics Service** if you want to track the external user transactions and click **Next**.

i. Optional Select the **XML Store** check box if you want XML Store, specify the following information, and click **Next**:

   - **XML Store Host**: Host name of the machine where BaseX server is installed and running.
   - **XML Store Port**: Port on which BaseX server is running.
   - **XML Store Administrator/Superuser password**: Password of the admin user in BaseX.
     - If HashiCorp Vault is enabled, the XML Store administrator/ superuser password is retrieved from the HashiCorp Vault server.
     - If HashiCorp Vault is not enabled, type the XML Store administrator/superuser password.

j. Specify the data file path for BaseX and click **Next**.

k. Provide the repository owner password and click **Next**.

   - If HashiCorp Vault is enabled, the repository owner password is retrieved from the HashiCorp Vault server.
   - If HashiCorp Vault is not enabled, type the repository owner password.

l. Select **Finish configuration** and click **Next**.

11. If you upgraded from an installation using FAST full-text indexing, and selected xPlore full-text indexing, you must restart Documentum CM Server again after you complete the Documentum CM Server configuration.

12. After you complete the Documentum CM Server configuration, create a nonunique index on the `dm_sysobject.r_object_id` and `r_aspect_name` properties by using the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dm_sysobject',
attribute='r_aspect_name',use_id_col=true
```

The inclusion of the use_id_col argument set to true automatically causes Documentum CM Server to include the r_object_id column in the index.

13. If you are upgrading a repository in a distributed environment that uses a Branch Office Caching Services and asynchronous write jobs, create an index on the `dmr_content_s` (`i_parked_state`, `r_object_id`) properties. Use the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dmr_content',
attribute='i_parked_state',use_id_col=true,id_in_front=false
```

5.7.3 Post-upgrade tasks

Follow the steps provided in "Post-upgrade tasks" on page 94.

5.8 Upgrading Documentum CM Server 21.1 to 25.4 – Linux/Oracle

The following table lists the base and upgraded versions of the Documentum CM Server, operating system, and database that are supported in this upgrade scenario:

Table 5-7: Base and upgraded OS/DB/Documentum CM Server versions

	Base version	Upgraded version
Operating System	Red Hat Enterprise Linux 8.0 (64-bit)	Red Hat Enterprise Linux 9.x (64-bit)
Database	Oracle 18.3	Oracle 23ai
Documentum CM Server	64-bit Documentum CM Server 21.1	64-bit Documentum CM Server 25.4

5.8.1 Pre-upgrade tasks

1. Review the "Upgrading Documentum CM Server" on page 35.
2. Back up the repository.
3. Optional Take a backup of all users that are part of the *Admin group*. In addition, ensure that you take the backup of the customized attribute like group_address.
4. If the repository contains customized repository formats (dm_format objects), back up the customized formats.
5. Temporarily increase the amount of rollback space available in the RDBMS. The number of rollback segments should be commensurate with the size of the repository and should be in segments of equal size. For the steps, refer to the database documentation.
6. Ensure that you have sufficient disk space on the computer hosting the database.
7. Run the Consistency Checker tool. The syntax is:

   ```
   dmbasic -fconsistency_checker.ebs -eEntry_Point -- <repository_name>
   <superuser> <password>
   ```

8. Fix the inconsistencies reported by the Consistency Checker tool as errors.
9. Ensure that the dm_server_config object is unlocked.
10. Ensure that you perform the tasks mentioned in step step 17 in "Upgrade checklist" on page 35.
11. If you want to upgrade AEK key, make sure that you update the AEK passphrase to comply with password complexity rules using the following command format:

    ```
    dm_crypto_change_passphrase.exe -keyname <name of aek key> -passphrase <old
    passsphrase> -newpassphrase <new password with complexity rules>
    ```

    For example:

    ```
    dm_crypto_change_passphrase.exe -keyname aek_name -passphrase Password@123 -
    newpassphrase Password@1234567890
    ```

    The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about password complexity rules.

    Note: This step is valid only when upgrading to a repository where HashiCorp Vault is not enabled.

12. If you want to upgrade AEK key in a repository where HashiCorp Vault is enabled, then you must create HashiCorp Vault-based AEK keys.

    OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD) contains detailed information.

5.8.2 Upgrade tasks

1. Upgrade the Linux operating system to Red Hat Enterprise Linux 9.x (64-bit).
2. Upgrade the Oracle database 18.3 to Oracle 19c, and then upgrade from Oracle 19c to Oracle 23ai.
3. Disable all jobs.
   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
   b. Right-click the job and select **Properties**.
   c. On the **Properties** page, set the **State** to `Inactive`.
4. Shut down the repositories and connection brokers.
   a. For each repository, run the `dm_shutdown_repository` script, where repository is the name of the Documentum CM Server to be stopped.
   b. Stop each connection broker using the `dm_stop_docbroker` utility on the command line:
   ```
   % dm_stop_docbroker [-Ppassword][-B[batch]] [-Nport_number][-Sservice_name]
   ```
5. To shut down the application server on Linux, stop the service called Java Method Server. Ensure that the application server does not start automatically after a host restart.

   Run the script `$DM_JMS_HOME/bin/stopMethodServer.sh`.
6. Download and install the supported version of Oracle JDK/OpenJDK version from Oracle JDK/OpenJDK website. The *Oracle JDK and OpenJDK* documentation contains detailed information. "Using SSL communication" on page 34 provides more information.
7. Run the random generator as root using the following command:
   ```
   /sbin/rngd -b -r /dev/urandom -o /dev/random
   ```

   Note: If the operating system is upgraded to Linux 7.x/8.x/9.x, then run the following command as root:
   ```
   ln -s /usr/lib64/libsasl2.so.3.0.0 /usr/lib64/libsasl2.so.2
   ```
8. Run the Documentum CM Server installation program.
   a. Run `serverSetup.bin`.

   Note: Before you install Documentum CM Server on Linux, ensure that you have completed the following tasks:

   - Install the Expect version 5.45.4 or earlier script utility.
   - Install the TCL version 8.6.8 or earlier script utility.

The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more details.

b. Click **Yes** when the installer displays a message stating that you are trying to upgrade the older version and asks if you want to proceed.

c. Accept the license agreement and click **Next**.

d. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

e. If you select the **Enable Vault** check box, provide the following information and click **Next**:

i. **DSIS URL**: Provide a value in the following format:

```
http://localhost:<port mentioned in application.properties>/dsis
```

ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

> **Important**
>
> If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

f. Browse and specify the directory where the supported version of JDK is installed. Click **Next**.

g. Set the administrator password and specify an available listening port for the embedded application server used by Documentum CM Server and click **Next**.

- **Admin User Password**: Application server password. You must follow the password complexity rules. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about the password complexity rules.
  - If HashiCorp Vault is enabled, then the application server password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, then type the application server password.
- **Listen Port**: The port on which the application server listens for standard administration connections. A total of 20 ports, starting from the one you specify is used by the application server, and all of them must be available. The default port number is 9080. Irrespective of you accepting the default port or choosing another one, do not change this port after the initial configuration.

h. Review the installation summary and click **Install** to begin installation.

i. To open the Documentum CM Server configuration program and configure the repository, select **Configure now** and click **Done**.

9. Upgrade the connection broker.

    a. Open the Documentum CM Server configuration program.
    b. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.
    c. If you select the **Enable Vault** check box, provide the following information and click **Next**:

        i. **DSIS URL**: Provide a value in the following format:

        ```
        http://localhost:<port mentioned in application.properties>/dsis
        ```

        ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

        Important

        If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

    d. Select **Connection broker** and click **Next**.
    e. Select **Upgrade a connection broker**.
    f. Select the connection broker to upgrade from the list and click **Next**.
    g. Complete the configuration, select **Perform additional configuration**, and click **Next**.

10. Upgrade the existing repository.

    a. On the configuration program options page, select **Repository** and then click **Next**.
    b. Select **Upgrade an existing repository**.
    c. Select the repository to upgrade from the list, and click **Next**.
    d. You can choose if you want to upgrade AEK key or continue with the existing AEK key. Take a backup of the AEK key. For creating new AEK key, refer to the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.
    e. Type the **Connection Broker Port** and **Connection Broker Host** and click **Next**.
    f. Select the **Connection Mode** for the repository and click **Next**. If you select the **Secure** or **Native and Secure** options, select **Use certificate** on the next page and provide the required details.

        If HashiCorp Vault is enabled, to prepare the certificate passwords, the contents of the `broker.pwd` and `server.pwd` files must be updated with the `<secret_name>/<key_name>`. For example:

        In the `broker.pwd` file:

        ```
        DOCBROKER_CERT_PASSWORD/<host name of connection broker>
        ```

        In the `server.pwd` file:

```
DOCBASE_CERT_PASSWORD/<repository name>
```

Click **Next**.

g. Select the type of mail server, perform the tasks depending on the mail server you select, and click **Next**. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.

h. Optional Select **Enable External User Metrics Service** if you want to track the external user transactions and click **Next**.

i. Optional Select the **XML Store** check box if you want XML Store, specify the following information, and click **Next**:

- **XML Store Host**: Host name of the machine where BaseX server is installed and running.
- **XML Store Port**: Port on which BaseX server is running.
- **XML Store Administrator/Superuser password**: Password of the admin user in BaseX.
  - If HashiCorp Vault is enabled, the XML Store administrator/ superuser password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, type the XML Store administrator/superuser password.

j. Specify the data file path for BaseX and click **Next**.

k. Provide the repository owner password and click **Next**.

- If HashiCorp Vault is enabled, the repository owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the repository owner password.

l. Select **Finish configuration** and click **Next**.

11. If you upgraded from an installation using FAST full-text indexing, and selected xPlore full-text indexing, you must restart Documentum CM Server again after you complete the Documentum CM Server configuration.

12. After you complete the Documentum CM Server configuration, create a nonunique index on the `dm_sysobject.r_object_id` and `r_aspect_name` properties by using the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dm_sysobject',
attribute='r_aspect_name',use_id_col=true
```

The inclusion of the use_id_col argument set to true automatically causes Documentum CM Server to include the r_object_id column in the index.

13. If you are upgrading a repository in a distributed environment that uses a Branch Office Caching Services and asynchronous write jobs, create an index on the `dmr_content_s` (`i_parked_state`, `r_object_id`) properties. Use the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dmr_content',
attribute='i_parked_state',use_id_col=true,id_in_front=false
```

5.8.3 Post-upgrade tasks

Follow the steps provided in "Post-upgrade tasks" on page 94.

5.9 Upgrading Documentum CM Server 21.2 to 25.4 – Windows/Oracle

The following table lists the base and upgraded versions of the Documentum CM Server, operating system, and database that are supported in this upgrade scenario:

Table 5-8: Base and upgraded OS/DB/Documentum CM Server versions

	Base version	Upgraded version
Operating System	Windows Server 2019 (64-bit)	Windows Server 2022 (64-bit)
Database	Oracle 18.3	Oracle 19c
Documentum CM Server	64-bit Documentum CM Server 21.2	64-bit Documentum CM Server 25.4

5.9.1 Pre-upgrade tasks

Note: To make the upgrade process work faster, if you use functional or bitmap Oracle customized indexes in Oracle database, then drop them prior to the upgrade and recreate them after the migration.

1. Review the "Upgrading Documentum CM Server" on page 35.
2. If you are installing the xPlore indexing server, review the *OpenText Documentum xPlore Installation Guide*.
3. Back up the repository.
4. Optional Take a backup of all users that are part of the *Admin group*. In addition, ensure that you take the backup of the customized attribute like group_address.
5. If the repository contains customized repository formats (dm_format objects), back up the customized formats.
6. Temporarily increase the amount of rollback space available in the RDBMS. The number of rollback segments should be commensurate with the size of the repository and should be in segments of equal size. For the steps, refer to the database documentation.
7. Ensure that you have sufficient disk space on the computer hosting the database.
8. Run the Consistency Checker tool. The syntax is:

```
dmbasic -fconsistency_checker.ebs -eEntry_Point -- <repository_name>
<superuser> <password>
```

9. Fix the inconsistencies reported by the Consistency Checker tool as errors.
10. Ensure that the dm_server_config object is unlocked.
11. If you want to upgrade AEK key, make sure that you update the AEK passphrase to comply with password complexity rules using the following command format:

    ```
    dm_crypto_change_passphrase.exe -keyname <name of aek key> -passphrase <old
    passsphrase> -newpassphrase <new password with complexity rules>
    ```

    For example:

    ```
    dm_crypto_change_passphrase.exe -keyname aek_name -passphrase Password@123 -
    newpassphrase Password@1234567890
    ```

    The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about password complexity rules.

    Note: This step is valid only when upgrading to a repository where HashiCorp Vault is not enabled.

12. If you want to upgrade AEK key in a repository where HashiCorp Vault is enabled, then you must create HashiCorp Vault-based AEK keys.

    OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD) contains detailed information.

5.9.2 Upgrade tasks

1. Upgrade the Windows operating system to Windows Server 2022 (64-bit).
2. Install the latest version of Microsoft Visual C++ 2013, 2019, and 2022 Redistributable (64-bit) package before upgrading a repository. This provides the correct operating system runtime libraries for the Documentum CM Server and other utilities.
3. Upgrade the database to Oracle 19c.
4. After you upgrade the database, create an `ORACLE_HOME` environment variable in Windows that points to the location of the 64-bit `tnsnames.ora` file. The entries from the 32-bit `tnsnames.ora` file have to be copied into the 64-bit `tnsnames.ora` file.
5. Disable all jobs.
   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
   b. Right-click the job and select **Properties**.
   c. On the **Properties** page, set the **State** to `Inactive`.

6. Shut down the repositories and connection brokers.

   a. Click **Start > Programs > Documentum > Server Manager**.
   b. Select the correct Documentum CM Server and click **Stop**.
   c. On the **Connection Broker** tab, select each connection broker, and then click **Stop**.

7. To shut down the application server on Windows, stop the service called Java Method Server. Ensure that the application server does not start automatically after a host restart.

   Click **Start > Control Panel > Administrative Tools > Services**, select the **Java Method Server**, and then click **Stop**.

8. During the upgrade from 32-bit to 64-bit, Documentum CM Server, you cannot upgrade the authentication plug-ins that you have installed. You need to replace the 32-bit authentication plug-ins with the 64-bit plug-ins. You can find the plug-ins in the `%DM_HOME%\install\external_apps\authplugins` folder.

9. Download and install the supported version of Oracle JDK/OpenJDK version from Oracle JDK/OpenJDK website. The *Oracle JDK and OpenJDK* documentation contains detailed information. "Using SSL communication" on page 34 provides more details about SSL communication with JDK.

10. Run the Documentum CM Server installation program.

    a. Run `serverSetup.exe`.
    b. Click **Yes** when the installer displays a message stating that you are trying to upgrade the older version and asks if you want to proceed.
    c. Accept the license agreement and click **Next**.
    d. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.
    e. If you select the **Enable Vault** check box, provide the following information and click **Next**:

       i. **DSIS URL**: Provide a value in the following format:

       ```
       http://localhost:<port mentioned in application.properties>/dsis
       ```

       ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

       Important

       If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

    f. On Windows, provide the installation owner password and click **Next**.

       - If HashiCorp Vault is enabled, the installation owner password is retrieved from the HashiCorp Vault server.

- If HashiCorp Vault is not enabled, type the installation owner password.

g. Browse and specify the directory where the supported version of JDK is installed. Click **Next**.

h. Set the administrator password and specify an available listening port for the embedded application server used by Documentum CM Server and click **Next**.

- **Admin User Password**: Application server password. You must follow the password complexity rules. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about the password complexity rules.
  - If HashiCorp Vault is enabled, then the application server password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, then type the application server password.
- **Listen Port**: The port on which the application server listens for standard administration connections. A total of 20 ports, starting from the one you specify is used by the application server, and all of them must be available. The default port number is 9080. Irrespective of you accepting the default port or choosing another one, do not change this port after the initial configuration.

i. Review the installation summary and click **Install** to begin installation.

j. To open the Documentum CM Server configuration program and configure the repository, select **Configure now** and click **Done**.

11. Upgrade the connection broker.

a. Open the Documentum CM Server configuration program.

b. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

c. If you select the **Enable Vault** check box, provide the following information and click **Next**:

i. **DSIS URL**: Provide a value in the following format:

```
http://localhost:<port mentioned in application.properties>/dsis
```

ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

> **Important**
> If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

d. Select **Connection broker** and click **Next**.

e. On Windows, provide the installation owner password and click **Next**.

- If HashiCorp Vault is enabled, the installation owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the installation owner password.

f. Select **Upgrade a connection broker**.

g. Select the connection broker to upgrade from the list and click **Next**.

h. Complete the configuration, select **Perform additional configuration**, and click **Next**.

12. Upgrade the existing repository.

a. On the configuration program options page, select **Repository** and then click **Next**.

b. Select **Upgrade an existing repository**.

c. Select the repository to upgrade from the list, and click **Next**.

d. You can choose if you want to upgrade AEK key or continue with the existing AEK key. Take a backup of the AEK key. For creating new AEK key, refer to the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

e. Type the **Connection Broker Port** and **Connection Broker Host** and click **Next**.

f. Select the **Connection Mode** for the repository and click **Next**. If you select the **Secure** or **Native and Secure** options, select **Use certificate** on the next page and provide the required details.

If HashiCorp Vault is enabled, to prepare the certificate passwords, the contents of the `broker.pwd` and `server.pwd` files must be updated with the `<secret_name>/<key_name>`. For example:

In the `broker.pwd` file:

```
DOCBROKER_CERT_PASSWORD/<host name of connection broker>
```

In the `server.pwd` file:

```
DOCBASE_CERT_PASSWORD/<repository name>
```

Click **Next**.

g. Select the type of mail server, perform the tasks depending on the mail server you select, and click **Next**. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.

h. Optional Select **Enable External User Metrics Service** if you want to track the external user transactions and click **Next**.

i. Optional Select the **XML Store** check box if you want XML Store, specify the following information, and click **Next**:

- **XML Store Host**: Host name of the machine where BaseX server is installed and running.

- **XML Store Port**: Port on which BaseX server is running.
- **XML Store Administrator/Superuser password**: Password of the admin user in BaseX.
  - If HashiCorp Vault is enabled, the XML Store administrator/ superuser password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, type the XML Store administrator/superuser password.

j. Specify the data file path for BaseX and click **Next**.

k. Provide the repository owner password and click **Next**.

- If HashiCorp Vault is enabled, the repository owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the repository owner password.

l. Select **Finish configuration** and click **Next**.

13. If you upgraded from an installation using FAST full-text indexing, and selected xPlore full-text indexing, you must restart Documentum CM Server again after you complete the Documentum CM Server configuration.

14. After you complete the Documentum CM Server configuration, create a nonunique index on the `dm_sysobject.r_object_id` and `r_aspect_name` properties by using the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dm_sysobject',
attribute='r_aspect_name',use_id_col=true
```

The inclusion of the use_id_col argument set to true automatically causes Documentum CM Server to include the r_object_id column in the index.

15. If you are upgrading a repository in a distributed environment that uses a Branch Office Caching Services and asynchronous write jobs, create an index on the `dmr_content_s` (`i_parked_state`, `r_object_id`) properties. Use the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dmr_content',
attribute='i_parked_state',use_id_col=true,id_in_front=false
```

5.9.3 Post-upgrade tasks

Follow the steps provided in "Post-upgrade tasks" on page 81.

5.10 Upgrading Documentum CM Server 21.3 to 25.4 – Linux/Oracle

The following table lists the base and upgraded versions of the Documentum CM Server, operating system, and database that are supported in this upgrade scenario:

Table 5-9: Base and upgraded OS/DB/Documentum CM Server versions

	Base version	Upgraded version
Operating System	Red Hat Enterprise Linux 8.3 (64-bit)	Red Hat Enterprise Linux 9.x (64-bit)
Database	Oracle 18.3	Oracle 19c
Documentum CM Server	64-bit Documentum CM Server 21.3	64-bit Documentum CM Server 25.4

5.10.1 Pre-upgrade tasks

1. Review the "Upgrading Documentum CM Server" on page 35.
2. Back up the repository.
3. Optional Take a backup of all users that are part of the *Admin group*. In addition, ensure that you take the backup of the customized attribute like group_address.
4. If the repository contains customized repository formats (dm_format objects), back up the customized formats.
5. Temporarily increase the amount of rollback space available in the RDBMS. The number of rollback segments should be commensurate with the size of the repository and should be in segments of equal size. For the steps, refer to the database documentation.
6. Ensure that you have sufficient disk space on the computer hosting the database.
7. Run the Consistency Checker tool. The syntax is:

```
dmbasic -fconsistency_checker.ebs -eEntry_Point -- <repository_name>
<superuser> <password>
```

8. Fix the inconsistencies reported by the Consistency Checker tool as errors.
9. Ensure that the dm_server_config object is unlocked.
10. Ensure that you perform the tasks mentioned in step step 17 in "Upgrade checklist" on page 35.
11. If you want to upgrade AEK key, make sure that you update the AEK passphrase to comply with password complexity rules using the following command format:

```
dm_crypto_change_passphrase.exe -keyname <name of aek key> -passphrase <old
passsphrase> -newpassphrase <new password with complexity rules>
```

For example:

```
dm_crypto_change_passphrase.exe -keyname aek_name -passphrase Password@123 -
newpassphrase Password@1234567890
```

The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about password complexity rules.

Note: This step is valid only when upgrading to a repository where HashiCorp Vault is not enabled.

12. If you want to upgrade AEK key in a repository where HashiCorp Vault is enabled, then you must create HashiCorp Vault-based AEK keys.

    OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD) contains detailed information.

5.10.2 Upgrade tasks

1. Upgrade the Linux operating system to Red Hat Enterprise Linux 9.x (64-bit).
2. Upgrade the database to Oracle 19c.
3. Disable all jobs.
   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
   b. Right-click the job and select **Properties**.
   c. On the **Properties** page, set the **State** to `Inactive`.
4. Shut down the repositories and connection brokers.
   a. For each repository, run the `dm_shutdown_repository` script, where repository is the name of the Documentum CM Server to be stopped.
   b. Stop each connection broker using the `dm_stop_docbroker` utility on the command line:

      ```
      % dm_stop_docbroker [-Ppassword][-B[batch]] [-Nport_number][-Sservice_name]
      ```
5. To shut down the application server on Linux, stop the service called Java Method Server. Ensure that the application server does not start automatically after a host restart.

   Run the script `$DM_JMS_HOME/bin/stopMethodServer.sh`.
6. Download and install the supported version of Oracle JDK/OpenJDK version from Oracle JDK/OpenJDK website. The *Oracle JDK and OpenJDK* documentation contains detailed information. "Using SSL communication" on page 34 provides more information.
7. Run the random generator as root using the following command:

```
/sbin/rngd -b -r /dev/urandom -o /dev/random
```

Note: If the operating system is upgraded to Linux 7.x/8.x/9.x, then run the following command as root:

```
ln -s /usr/lib64/libsasl2.so.3.0.0 /usr/lib64/libsasl2.so.2
```

8. Run the Documentum CM Server installation program.

   a. Run `serverSetup.bin`.

      Note: Before you install Documentum CM Server on Linux, ensure that you have completed the following tasks:

      - Install the Expect version 5.45.4 or earlier script utility.
      - Install the TCL version 8.6.8 or earlier script utility.

      The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more details.

   b. Click **Yes** when the installer displays a message stating that you are trying to upgrade the older version and asks if you want to proceed.

   c. Accept the license agreement and click **Next**.

   d. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

   e. If you select the **Enable Vault** check box, provide the following information and click **Next**:

      i. **DSIS URL**: Provide a value in the following format:

      ```
      http://localhost:<port mentioned in application.properties>/dsis
      ```

      ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

      Important

      If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

   f. Browse and specify the directory where the supported version of JDK is installed. Click **Next**.

   g. Set the administrator password and specify an available listening port for the embedded application server used by Documentum CM Server and click **Next**.

      - **Admin User Password**: Application server password. You must follow the password complexity rules. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide*

(EDCSY250400-IGD) contains detailed information about the password complexity rules.

  - If HashiCorp Vault is enabled, then the application server password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, then type the application server password.

- **Listen Port**: The port on which the application server listens for standard administration connections. A total of 20 ports, starting from the one you specify is used by the application server, and all of them must be available. The default port number is 9080. Irrespective of you accepting the default port or choosing another one, do not change this port after the initial configuration.

h. Review the installation summary and click **Install** to begin installation.

i. To open the Documentum CM Server configuration program and configure the repository, select **Configure now** and click **Done**.

9. Upgrade the connection broker.

   a. Open the Documentum CM Server configuration program.

   b. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

   c. If you select the **Enable Vault** check box, provide the following information and click **Next**:

      i. **DSIS URL**: Provide a value in the following format:

      ```
      http://localhost:<port mentioned in application.properties>/dsis
      ```

      ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

      Important

      If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

   d. Select **Connection broker** and click **Next**.

   e. Select **Upgrade a connection broker**.

   f. Select the connection broker to upgrade from the list and click **Next**.

   g. Complete the configuration, select **Perform additional configuration**, and click **Next**.

10. Upgrade the existing repository.

    a. On the configuration program options page, select **Repository** and then click **Next**.

    b. Select **Upgrade an existing repository**.

c. Select the repository to upgrade from the list, and click **Next**.

d. You can choose if you want to upgrade AEK key or continue with the existing AEK key. Take a backup of the AEK key. For creating new AEK key, refer to the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

e. Type the **Connection Broker Port** and **Connection Broker Host** and click **Next**.

f. Select the **Connection Mode** for the repository and click **Next**. If you select the **Secure** or **Native and Secure** options, select **Use certificate** on the next page and provide the required details.

   If HashiCorp Vault is enabled, to prepare the certificate passwords, the contents of the `broker.pwd` and `server.pwd` files must be updated with the `<secret_name>/<key_name>`. For example:

   In the `broker.pwd` file:

   ```
   DOCBROKER_CERT_PASSWORD/<host name of connection broker>
   ```

   In the `server.pwd` file:

   ```
   DOCBASE_CERT_PASSWORD/<repository name>
   ```

   Click **Next**.

g. Select the type of mail server, perform the tasks depending on the mail server you select, and click **Next**. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.

h. Optional Select **Enable External User Metrics Service** if you want to track the external user transactions and click **Next**.

i. Optional Select the **XML Store** check box if you want XML Store, specify the following information, and click **Next**:

   - **XML Store Host**: Host name of the machine where BaseX server is installed and running.
   - **XML Store Port**: Port on which BaseX server is running.
   - **XML Store Administrator/Superuser password**: Password of the admin user in BaseX.
     - If HashiCorp Vault is enabled, the XML Store administrator/ superuser password is retrieved from the HashiCorp Vault server.
     - If HashiCorp Vault is not enabled, type the XML Store administrator/superuser password.

j. Specify the data file path for BaseX and click **Next**.

k. Provide the repository owner password and click **Next**.

   - If HashiCorp Vault is enabled, the repository owner password is retrieved from the HashiCorp Vault server.
   - If HashiCorp Vault is not enabled, type the repository owner password.

l. Select **Finish configuration** and click **Next**.

11. If you upgraded from an installation using FAST full-text indexing, and selected xPlore full-text indexing, you must restart Documentum CM Server again after you complete the Documentum CM Server configuration.

12. After you complete the Documentum CM Server configuration, create a nonunique index on the `dm_sysobject.r_object_id` and `r_aspect_name` properties by using the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dm_sysobject',
attribute='r_aspect_name',use_id_col=true
```

The inclusion of the use_id_col argument set to true automatically causes Documentum CM Server to include the r_object_id column in the index.

13. If you are upgrading a repository in a distributed environment that uses a Branch Office Caching Services and asynchronous write jobs, create an index on the `dmr_content_s` (`i_parked_state`, `r_object_id`) properties. Use the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dmr_content',
attribute='i_parked_state',use_id_col=true,id_in_front=false
```

5.10.3 Post-upgrade tasks

Follow the steps provided in "Post-upgrade tasks" on page 94.

5.11 Upgrading Documentum CM Server 21.4 to 25.4 – Linux/Oracle

The following table lists the base and upgraded versions of the Documentum CM Server, operating system, and database that are supported in this upgrade scenario:

Table 5-10: Base and upgraded OS/DB/Documentum CM Server versions

	Base version	Upgraded version
Operating System	Red Hat Enterprise Linux 7.9 (64-bit)	Red Hat Enterprise Linux 8.10 (64-bit)
Database	Oracle 19c	Oracle 23ai
Documentum CM Server	64-bit Documentum CM Server 21.4	64-bit Documentum CM Server 25.4

5.11.1 Pre-upgrade tasks

1. Review the "Upgrading Documentum CM Server" on page 35.
2. Back up the repository.
3. Optional Take a backup of all users that are part of the *Admin group*. In addition, ensure that you take the backup of the customized attribute like group_address.
4. If the repository contains customized repository formats (dm_format objects), back up the customized formats.
5. Temporarily increase the amount of rollback space available in the RDBMS. The number of rollback segments should be commensurate with the size of the repository and should be in segments of equal size. For the steps, refer to the database documentation.
6. Ensure that you have sufficient disk space on the computer hosting the database.
7. Run the Consistency Checker tool. The syntax is:

   ```
   dmbasic -fconsistency_checker.ebs -eEntry_Point -- <repository_name>
   <superuser> <password>
   ```

8. Fix the inconsistencies reported by the Consistency Checker tool as errors.
9. Ensure that the dm_server_config object is unlocked.
10. Ensure that you perform the tasks mentioned in step step 17 in "Upgrade checklist" on page 35.
11. If you want to upgrade AEK key, make sure that you update the AEK passphrase to comply with password complexity rules using the following command format:

    ```
    dm_crypto_change_passphrase.exe -keyname <name of aek key> -passphrase <old
    passsphrase> -newpassphrase <new password with complexity rules>
    ```

    For example:

    ```
    dm_crypto_change_passphrase.exe -keyname aek_name -passphrase Password@123 -
    newpassphrase Password@1234567890
    ```

    The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about password complexity rules.

    Note: This step is valid only when upgrading to a repository where HashiCorp Vault is not enabled.

12. If you want to upgrade AEK key in a repository where HashiCorp Vault is enabled, then you must create HashiCorp Vault-based AEK keys.

    OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD) contains detailed information.

5.11.2 Upgrade tasks

1. Upgrade the Linux operating system to Red Hat Enterprise Linux 8.10 (64-bit).
2. Upgrade the database to Oracle 23ai.
3. Disable all jobs.
   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
   b. Right-click the job and select **Properties**.
   c. On the **Properties** page, set the **State** to `Inactive`.
4. Shut down the repositories and connection brokers.
   a. For each repository, run the `dm_shutdown_repository` script, where repository is the name of the Documentum CM Server to be stopped.
   b. Stop each connection broker using the `dm_stop_docbroker` utility on the command line:
   ```
   % dm_stop_docbroker [-Ppassword][-B[batch]] [-Nport_number][-Sservice_name]
   ```
5. To shut down the application server on Linux, stop the service called Java Method Server. Ensure that the application server does not start automatically after a host restart.

   Run the script `$DM_JMS_HOME/bin/stopMethodServer.sh`.
6. Download and install the supported version of Oracle JDK/OpenJDK version from Oracle JDK/OpenJDK website. The *Oracle JDK and OpenJDK* documentation contains detailed information. "Using SSL communication" on page 34 provides more information.
7. Run the random generator as root using the following command:
   ```
   /sbin/rngd -b -r /dev/urandom -o /dev/random
   ```

   Note: If the operating system is upgraded to Linux 7.x/8.x/9.x, then run the following command as root:
   ```
   ln -s /usr/lib64/libsasl2.so.3.0.0 /usr/lib64/libsasl2.so.2
   ```
8. Run the Documentum CM Server installation program.
   a. Run `serverSetup.bin`.

      Note: Before you install Documentum CM Server on Linux, ensure that you have completed the following tasks:

      - Install the Expect version 5.45.4 or earlier script utility.
      - Install the TCL version 8.6.8 or earlier script utility.

The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more details.

b. Click **Yes** when the installer displays a message stating that you are trying to upgrade the older version and asks if you want to proceed.

c. Accept the license agreement and click **Next**.

d. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

e. If you select the **Enable Vault** check box, provide the following information and click **Next**:

i. **DSIS URL**: Provide a value in the following format:

```
http://localhost:<port mentioned in application.properties>/dsis
```

ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

> **Important**
>
> If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from HashiCorp Vault. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

f. Browse and specify the directory where the supported version of JDK is installed. Click **Next**.

g. Set the administrator password and specify an available listening port for the embedded application server used by Documentum CM Server and click **Next**.

- **Admin User Password**: Application server password. You must follow the password complexity rules. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about the password complexity rules.
  - If HashiCorp Vault is enabled, then the application server password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, then type the application server password.
- **Listen Port**: The port on which the application server listens for standard administration connections. A total of 20 ports, starting from the one you specify is used by the application server, and all of them must be available. The default port number is 9080. Irrespective of you accepting the default port or choosing another one, do not change this port after the initial configuration.

h. Review the installation summary and click **Install** to begin installation.

i. To open the Documentum CM Server configuration program and configure the repository, select **Configure now** and click **Done**.

9. Upgrade the connection broker.

    a. Open the Documentum CM Server configuration program.
    b. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.
    c. If you select the **Enable Vault** check box, provide the following information and click **Next**:

        i. **DSIS URL**: Provide a value in the following format:

        ```
        http://localhost:<port mentioned in application.properties>/dsis
        ```

        ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

        Important

        If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

    d. Select **Connection broker** and click **Next**.
    e. Select **Upgrade a connection broker**.
    f. Select the connection broker to upgrade from the list and click **Next**.
    g. Complete the configuration, select **Perform additional configuration**, and click **Next**.

10. Upgrade the existing repository.

    a. On the configuration program options page, select **Repository** and then click **Next**.
    b. Select **Upgrade an existing repository**.
    c. Select the repository to upgrade from the list, and click **Next**.
    d. You can choose if you want to upgrade AEK key or continue with the existing AEK key. Take a backup of the AEK key. For creating new AEK key, refer to the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.
    e. Type the **Connection Broker Port** and **Connection Broker Host** and click **Next**.
    f. Select the **Connection Mode** for the repository and click **Next**. If you select the **Secure** or **Native and Secure** options, select **Use certificate** on the next page and provide the required details.

        If HashiCorp Vault is enabled, to prepare the certificate passwords, the contents of the `broker.pwd` and `server.pwd` files must be updated with the `<secret_name>/<key_name>`. For example:

        In the `broker.pwd` file:

        ```
        DOCBROKER_CERT_PASSWORD/<host name of connection broker>
        ```

        In the `server.pwd` file:

```
DOCBASE_CERT_PASSWORD/<repository name>
```

Click **Next**.

g. Select the type of mail server, perform the tasks depending on the mail server you select, and click **Next**. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.

h. Optional Select **Enable External User Metrics Service** if you want to track the external user transactions and click **Next**.

i. Optional Select the **XML Store** check box if you want XML Store, specify the following information, and click **Next**:

- **XML Store Host**: Host name of the machine where BaseX server is installed and running.
- **XML Store Port**: Port on which BaseX server is running.
- **XML Store Administrator/Superuser password**: Password of the admin user in BaseX.
  - If HashiCorp Vault is enabled, the XML Store administrator/superuser password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, type the XML Store administrator/superuser password.

j. Specify the data file path for BaseX and click **Next**.

k. Provide the repository owner password and click **Next**.

- If HashiCorp Vault is enabled, the repository owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the repository owner password.

l. Select **Finish configuration** and click **Next**.

11. If you upgraded from an installation using FAST full-text indexing, and selected xPlore full-text indexing, you must restart Documentum CM Server again after you complete the Documentum CM Server configuration.

12. After you complete the Documentum CM Server configuration, create a nonunique index on the `dm_sysobject.r_object_id` and `r_aspect_name` properties by using the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dm_sysobject',
attribute='r_aspect_name',use_id_col=true
```

The inclusion of the use_id_col argument set to true automatically causes Documentum CM Server to include the r_object_id column in the index.

13. If you are upgrading a repository in a distributed environment that uses a Branch Office Caching Services and asynchronous write jobs, create an index on the `dmr_content_s` (`i_parked_state`, `r_object_id`) properties. Use the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dmr_content',
attribute='i_parked_state',use_id_col=true,id_in_front=false
```

5.11.3 Post-upgrade tasks

Follow the steps provided in "Post-upgrade tasks" on page 94.

5.12 Upgrading Documentum CM Server 22.1 to 25.4 – Linux/Oracle

The following table lists the base and upgraded versions of the Documentum CM Server, operating system, and database that are supported in this upgrade scenario:

Table 5-11: Base and upgraded OS/DB/Documentum CM Server versions

	Base version	Upgraded version
Operating System	Red Hat Enterprise Linux 8.5 (64-bit)	Red Hat Enterprise Linux 9.x (64-bit)
Database	Oracle 19c	Oracle 23ai
Documentum CM Server	64-bit Documentum CM Server 22.1	64-bit Documentum CM Server 25.4

5.12.1 Pre-upgrade tasks

1. Review the "Upgrading Documentum CM Server" on page 35.
2. Back up the repository.
3. Optionally, you can take a backup of all users that are part of the *Admin group*. In addition, ensure that you take the backup of the customized attribute like group_address.
4. If the repository contains customized repository formats (dm_format objects), back up the customized formats.
5. Temporarily increase the amount of rollback space available in the RDBMS. The number of rollback segments should be commensurate with the size of the repository and should be in segments of equal size. For the steps, refer to the database documentation.
6. Ensure that you have sufficient disk space on the computer hosting the database.
7. Run the Consistency Checker tool. The syntax is:

```
dmbasic -fconsistency_checker.ebs -eEntry_Point -- <repository_name>
<superuser> <password>
```

8. Fix the inconsistencies reported by the Consistency Checker tool as errors.

9. Ensure that the dm_server_config object is unlocked.
10. Ensure that you perform the tasks mentioned in step step 17 in "Upgrade checklist" on page 35.
11. If you want to upgrade AEK key, make sure that you update the AEK passphrase to comply with password complexity rules using the following command format:

```
dm_crypto_change_passphrase.exe -keyname <name of aek key> -passphrase <old
passsphrase> -newpassphrase <new password with complexity rules>
```

For example:

```
dm_crypto_change_passphrase.exe -keyname aek_name -passphrase Password@123 -
newpassphrase Password@1234567890
```

The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about password complexity rules.

Note: This step is valid only when upgrading to a repository where HashiCorp Vault is not enabled.

12. If you want to upgrade AEK key in a repository where HashiCorp Vault is enabled, then you must create HashiCorp Vault-based AEK keys.

OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD) contains detailed information.

5.12.2 Upgrade tasks

1. Upgrade the Linux operating system to Red Hat Enterprise Linux 9.x (64-bit).
2. Upgrade the database to Oracle 23ai.
3. Disable all jobs.
   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
   b. Right-click the job and select **Properties**.
   c. On the **Properties** page, set the **State** to `Inactive`.
4. Shut down the repositories and connection brokers.
   a. For each repository, run the `dm_shutdown_repository` script, where repository is the name of the Documentum CM Server to be stopped.
   b. Stop each connection broker using the `dm_stop_docbroker` utility on the command line:

```
% dm_stop_docbroker [-Ppassword][-B[batch]] [-Nport_number][-Sservice_name]
```

5. To shut down the application server on Linux, stop the service called Java Method Server. Ensure that the application server does not start automatically after a host restart.

Run the `$DM_JMS_HOME/bin/stopMethodServer.sh` script.

6. Download and install the supported version of Oracle JDK/OpenJDK version from Oracle JDK/OpenJDK website. The *Oracle JDK and OpenJDK* documentation contains detailed information. "Using SSL communication" on page 34 provides more details about SSL communication with JDK.
7. Run the random generator as root using the following command:

```
/sbin/rngd -b -r /dev/urandom -o /dev/random
```

Note: If the operating system is upgraded to Linux 7.x/8.x, then run the following command as root:

```
ln -s /usr/lib64/libsasl2.so.3.0.0 /usr/lib64/libsasl2.so.2
```

8. Run the Documentum CM Server installation program.
   a. Run `serverSetup.bin`.

      Note: Before you install Documentum CM Server on Linux, ensure that you have completed the following tasks:

      - Install the Expect version 5.45.4 or earlier script utility.
      - Install the TCL version 8.6.8 or earlier script utility.

      The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more details.
   b. Click **Yes** when the installer displays a message stating that you are trying to upgrade the older version and asks if you want to proceed.
   c. Accept the license agreement and click **Next**.
   d. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.
   e. If you select the **Enable Vault** check box, provide the following information and click **Next**:
      i. **DSIS URL**: Provide a value in the following format:

```
http://localhost:<port mentioned in application.properties>/dsis
```

      ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

      Important

      If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.
   f. Browse and specify the directory where the supported version of JDK is installed. Click **Next**.

g. Set the administrator password and specify an available listening port for the embedded application server used by Documentum CM Server and click **Next**.

- **Admin User Password**: Application server password. You must follow the password complexity rules. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about the password complexity rules.
  - If HashiCorp Vault is enabled, then the application server password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, then type the application server password.
- **Listen Port**: The port on which the application server listens for standard administration connections. A total of 20 ports, starting from the one you specify is used by the application server, and all of them must be available. The default port number is 9080. Irrespective of you accepting the default port or choosing another one, do not change this port after the initial configuration.

h. Review the installation summary and click **Install** to begin installation.

i. To open the Documentum CM Server configuration program and configure the repository, select **Configure now** and click **Done**.

9. Upgrade the connection broker.

a. Open the Documentum CM Server configuration program.

b. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

c. If you select the **Enable Vault** check box, provide the following information and click **Next**:

i. **DSIS URL**: Provide a value in the following format:

```
http://localhost:<port mentioned in application.properties>/dsis
```

ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

> **Important**
> If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

d. Select **Connection broker** and click **Next**.

e. Select **Upgrade a connection broker**.

f. Select the connection broker to upgrade from the list and click **Next**.

g. Complete the configuration, select **Perform additional configuration**, and click **Next**.

10. Upgrade the existing repository.

    a. On the configuration program options page, select **Repository** and then click **Next**.

    b. Select **Upgrade an existing repository**.

    c. Select the repository to upgrade from the list, and click **Next**.

    d. You can choose if you want to upgrade AEK key or continue with the existing AEK key. Take a backup of the AEK key. For creating new AEK key, refer to the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

    e. Type the **Connection Broker Port** and **Connection Broker Host** and click **Next**.

    f. Select the **Connection Mode** for the repository and click **Next**. If you select the **Secure** or **Native and Secure** options, select **Use certificate** on the next page and provide the required details.

    If HashiCorp Vault is enabled, to prepare the certificate passwords, the contents of the `broker.pwd` and `server.pwd` files must be updated with the `<secret_name>/<key_name>`. For example:

    In the `broker.pwd` file:

    ```
    DOCBROKER_CERT_PASSWORD/<host name of connection broker>
    ```

    In the `server.pwd` file:

    ```
    DOCBASE_CERT_PASSWORD/<repository name>
    ```

    Click **Next**.

    g. Select the type of mail server, perform the tasks depending on the mail server you select, and click **Next**. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.

    h. Optional Select **Enable External User Metrics Service** if you want to track the external user transactions and click **Next**.

    i. Optional Select the **XML Store** check box if you want XML Store, specify the following information, and click **Next**:

    - **XML Store Host**: Host name of the machine where BaseX server is installed and running.
    - **XML Store Port**: Port on which BaseX server is running.
    - **XML Store Administrator/Superuser password**: Password of the admin user in BaseX.
      - If HashiCorp Vault is enabled, the XML Store administrator/ superuser password is retrieved from the HashiCorp Vault server.
      - If HashiCorp Vault is not enabled, type the XML Store administrator/superuser password.

    j. Specify the data file path for BaseX and click **Next**.

k. Provide the repository owner password and click **Next**.

- If HashiCorp Vault is enabled, the repository owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the repository owner password.

l. Select **Finish configuration** and click **Next**.

11. If you upgraded from an installation using FAST full-text indexing, and selected xPlore full-text indexing, you must restart Documentum CM Server again after you complete the Documentum CM Server configuration.

12. After you complete the Documentum CM Server configuration, create a nonunique index on the `dm_sysobject.r_object_id` and `r_aspect_name` properties by using the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dm_sysobject',
attribute='r_aspect_name',use_id_col=true
```

The inclusion of the use_id_col argument set to true automatically causes Documentum CM Server to include the r_object_id column in the index.

13. If you are upgrading a repository in a distributed environment that uses a Branch Office Caching Services and asynchronous write jobs, create an index on the `dmr_content_s` (`i_parked_state`, `r_object_id`) properties. Use the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dmr_content',
attribute='i_parked_state',use_id_col=true,id_in_front=false
```

5.12.3 Post-upgrade tasks

Follow the steps provided in "Post-upgrade tasks" on page 94.

5.13 Upgrading Documentum CM Server 22.2 to 25.4 – Windows/SQL Server

The following table lists the base and upgraded versions of the Documentum CM Server, operating system, and database that are supported in this upgrade scenario:

Table 5-12: Base and upgraded OS/DB/Documentum CM Server versions

	Base version	Upgraded version
Operating System	Windows Server 2019 (64-bit)	Windows Server 2022 (64-bit)
Database	SQL Server 2017	SQL Server 2019
Documentum CM Server	64-bit Documentum CM Server 22.2	64-bit Documentum CM Server 25.4

5.13.1 Pre-upgrade tasks

1. Review the "Upgrading Documentum CM Server" on page 35.
2. Back up the repository.
3. Ensure that you apply the latest Documentum CM Server patch.
4. Optional Take a backup of all users that are part of the *Admin group*. In addition, ensure that you take the backup of the customized attribute like group_address.
5. If the repository contains customized repository formats (dm_format objects), back up the customized formats.
6. Temporarily increase the amount of rollback space available in the RDBMS. The number of rollback segments should be commensurate with the size of the repository and should be in segments of equal size. For the steps, refer to the database documentation.
7. Ensure that you have sufficient disk space on the computer hosting the database.
8. Run the Consistency Checker tool. The syntax is:

```
dmbasic -fconsistency_checker.ebs -eEntry_Point -- <repository_name>
<superuser> <password>
```

9. Fix the inconsistencies reported by the Consistency Checker tool as errors.
10. Ensure that the dm_server_config object is unlocked.
11. Optional If you are upgrading Documentum CM Server enabled with SSL communication and lockbox, perform the following tasks:
    a. Remove the key from the lockbox using the following example command format:

```
dm_crypto_create -lockbox lockbox.lb -lockboxpassphrase Password@123 -keyname
CSaek -removelockbox -output CSaek
```

    b. Comment the `crypto_lockbox` section from all the `docbroker.ini` and `server.ini` files.
    c. Restart the connection broker and the repository and ensure that they start properly.
12. If you want to upgrade AEK key, make sure that you update the AEK passphrase to comply with password complexity rules using the following command format:

```
dm_crypto_change_passphrase.exe -keyname <name of aek key> -passphrase <old
passsphrase> -newpassphrase <new password with complexity rules>
```

    For example:

```
dm_crypto_change_passphrase.exe -keyname aek_name -passphrase Password@123 -
newpassphrase Password@1234567890
```

The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about password complexity rules.

Note: This step is valid only when upgrading to a repository where HashiCorp Vault is not enabled.

13. If you want to upgrade AEK key in a repository where HashiCorp Vault is enabled, then you must create HashiCorp Vault-based AEK keys.

    OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD) contains detailed information.

5.13.2 Upgrade tasks

1. Upgrade the Windows operating system to Windows Server 2022 (64-bit).
2. Install the latest version of Microsoft Visual C++ 2013, 2019, and 2022 Redistributable (64-bit) package before upgrading a repository. This provides the correct operating system runtime libraries for the Documentum CM Server and other utilities.
3. Upgrade the database to SQL Server 2019 for Microsoft Windows with latest cumulative update.
4. Disable all jobs.
   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
   b. Right-click the job and select **Properties**.
   c. On the **Properties** page, set the **State** to `Inactive`.
5. Shut down the repositories and connection brokers.
   a. Click **Start > Programs > Documentum > Server Manager**.
   b. Select the correct Documentum CM Server and click **Stop**.
   c. On the **Connection Broker** tab, select each connection broker, and then click **Stop**.
6. To shut down the application server on Windows, stop the service called Java Method Server. Ensure that the application server does not start automatically after a host restart.

   Click **Start > Control Panel > Administrative Tools > Services**, select the **Java Method Server**, and then click **Stop**.
7. Download and install the supported version of Oracle JDK/OpenJDK version from Oracle JDK/OpenJDK website. The *Oracle JDK and OpenJDK* documentation contains detailed information. "Using SSL communication" on page 34 provides more details about SSL communication with JDK.
8. Run the Documentum CM Server installation program.

a. Run `serverSetup.exe`.

b. Click **Yes** when the installer displays a message stating that you are trying to upgrade the older version and asks if you want to proceed.

c. Accept the license agreement and click **Next**.

d. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

e. If you select the **Enable Vault** check box, provide the following information and click **Next**:

   i. **DSIS URL**: Provide a value in the following format:

   ```
   http://localhost:<port mentioned in application.properties>/dsis
   ```

   ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

   Important

   If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

f. On Windows, provide the installation owner password and click **Next**.

   - If HashiCorp Vault is enabled, the installation owner password is retrieved from the HashiCorp Vault server.
   - If HashiCorp Vault is not enabled, type the installation owner password.

g. Browse and specify the directory where the supported version of JDK is installed. Click **Next**.

h. Set the administrator password and specify an available listening port for the embedded application server used by Documentum CM Server and click **Next**.

   - **Admin User Password**: Application server password. You must follow the password complexity rules. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about the password complexity rules.
     - If HashiCorp Vault is enabled, then the application server password is retrieved from the HashiCorp Vault server.
     - If HashiCorp Vault is not enabled, then type the application server password.
   - **Listen Port**: The port on which the application server listens for standard administration connections. A total of 20 ports, starting from the one you specify is used by the application server, and all of them must be available. The default port number is 9080. Irrespective of you

accepting the default port or choosing another one, do not change this port after the initial configuration.

i. Review the installation summary and click **Install** to begin installation.

j. To open the Documentum CM Server configuration program and configure the repository, select **Configure now** and click **Done**.

9. Upgrade the connection broker.

a. Open the Documentum CM Server configuration program.

b. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

c. If you select the **Enable Vault** check box, provide the following information and click **Next**:

i. **DSIS URL**: Provide a value in the following format:

```
http://localhost:<port mentioned in application.properties>/dsis
```

ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

> **Important**
> If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

d. Select **Connection broker** and click **Next**.

e. On Windows, provide the installation owner password and click **Next**.

- If HashiCorp Vault is enabled, the installation owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the installation owner password.

f. Select **Upgrade a connection broker**.

g. Select the connection broker to upgrade from the list and click **Next**.

h. Complete the configuration, select **Perform additional configuration**, and click **Next**.

10. Upgrade the existing repository.

a. On the configuration program options page, select **Repository** and then click **Next**.

b. Select **Upgrade an existing repository**.

c. Select the repository to upgrade from the list, and click **Next**.

d. For creating new AEK key or use existing AEK key, refer to the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

e. Type the **Connection Broker Port** and **Connection Broker Host** and click **Next**.

f. Select the **Connection Mode** for the repository and click **Next**. If you select the **Secure** or **Native and Secure** options, select **Use certificate** on the next page and provide the required details.

If HashiCorp Vault is enabled, to prepare the certificate passwords, the contents of the `broker.pwd` and `server.pwd` files must be updated with the `<secret_name>/<key_name>`. For example:

In the `broker.pwd` file:

```
DOCBROKER_CERT_PASSWORD/<host name of connection broker>
```

In the `server.pwd` file:

```
DOCBASE_CERT_PASSWORD/<repository name>
```

Click **Next**.

g. Select the type of mail server, perform the tasks depending on the mail server you select, and click **Next**. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.

h. Optional Select **Enable External User Metrics Service** if you want to track the external user transactions and click **Next**.

i. Optional Select the **XML Store** check box if you want XML Store, specify the following information, and click **Next**:

- **XML Store Host**: Host name of the machine where BaseX server is installed and running.
- **XML Store Port**: Port on which BaseX server is running.
- **XML Store Administrator/Superuser password**: Password of the admin user in BaseX.
  - If HashiCorp Vault is enabled, the XML Store administrator/superuser password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, type the XML Store administrator/superuser password.

j. Specify the data file path for BaseX and click **Next**.

k. Provide the repository owner password and click **Next**.

- If HashiCorp Vault is enabled, the repository owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the repository owner password.

l. Select **Finish configuration** and click **Next**.

11. If you upgraded from an installation using FAST full-text indexing, and selected xPlore full-text indexing, you must restart Documentum CM Server again after you complete the Documentum CM Server configuration.

12. After you complete the Documentum CM Server configuration, create a nonunique index on the `dm_sysobject.r_object_id` and `r_aspect_name` properties by using the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dm_sysobject',
attribute='r_aspect_name',use_id_col=true
```

    The inclusion of the use_id_col argument set to true automatically causes Documentum CM Server to include the r_object_id column in the index.

13. If you are upgrading a repository in a distributed environment that uses a Branch Office Caching Services and asynchronous write jobs, create an index on the `dmr_content_s` (`i_parked_state`, `r_object_id`) properties. Use the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dmr_content',
attribute='i_parked_state',use_id_col=true,id_in_front=false
```

5.13.3 Post-upgrade tasks

Follow the steps provided in "Post-upgrade tasks" on page 81.

5.14 Upgrading Documentum CM Server 22.4 to 25.4 – Linux/PostgreSQL

The following table lists the base and upgraded versions of the Documentum CM Server, operating system, and database that are supported in this upgrade scenario:

Table 5-13: Base and upgraded OS/DB/Documentum CM Server versions

	Base version	Upgraded version
Operating System	Red Hat Enterprise Linux 7.x (64-bit)	Red Hat Enterprise Linux 9.x (64-bit)
Database	PostgreSQL 12	PostgreSQL 16
Documentum CM Server	64-bit Documentum CM Server 22.4	64-bit Documentum CM Server 25.4

5.14.1 Pre-upgrade tasks

1. Review the "Upgrading Documentum CM Server" on page 35.
2. Back up the repository.
3. Ensure that you apply the latest Documentum CM Server patch.
4. Optional Take a backup of all users that are part of the *Admin group*. In addition, ensure that you take the backup of the customized attribute like group_address.
5. If the repository contains customized repository formats (dm_format objects), back up the customized formats.

6. Run the Consistency Checker tool. The syntax is:

```
dmbasic -fconsistency_checker.ebs -eEntry_Point -- <repository_name>
<superuser> <password>
```

7. Fix the inconsistencies reported by the Consistency Checker tool as errors.
8. Ensure that the dm_server_config object is unlocked.
9. Ensure that you perform the tasks mentioned in step step 17 in "Upgrade checklist" on page 35.
10. If you want to upgrade AEK key, make sure that you update the AEK passphrase to comply with password complexity rules using the following command format:

```
dm_crypto_change_passphrase.exe -keyname <name of aek key> -passphrase <old
passsphrase> -newpassphrase <new password with complexity rules>
```

For example:

```
dm_crypto_change_passphrase.exe -keyname aek_name -passphrase Password@123 -
newpassphrase Password@1234567890
```

The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about password complexity rules.

Note: This step is valid only when upgrading to a repository where HashiCorp Vault is not enabled.

11. If you want to upgrade AEK key in a repository where HashiCorp Vault is enabled, then you must create HashiCorp Vault-based AEK keys.

OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD) contains detailed information.

5.14.2 Upgrade tasks

1. Upgrade the Linux operating system to Red Hat Enterprise Linux 8.x (64-bit).
2. Upgrade the Red Hat Enterprise Linux 8.x (64-bit) to Red Hat Enterprise Linux 9.x (64-bit).
3. Upgrade the database to PostgreSQL 16.
4. Disable all jobs.
   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
   b. Right-click the job and select **Properties**.
   c. On the **Properties** page, set the **State** to `Inactive`.
5. Shut down the repositories and connection brokers.
   a. For each repository, run the `dm_shutdown_repository` script, where repository is the name of the Documentum CM Server to be stopped.

b. Stop each connection broker using the `dm_stop_docbroker` utility on the command line:

```
% dm_stop_docbroker [-Ppassword][-B[batch]] [-Nport_number][-Sservice_name]
```

6. To shut down the application server on Linux, stop the service called Java Method Server. Ensure that the application server does not start automatically after a host restart.

   Run the script `$DM_JMS_HOME/bin/stopMethodServer.sh`.

7. Download and install the supported version of Oracle JDK/OpenJDK version from Oracle JDK/OpenJDK website. The *Oracle JDK and OpenJDK* documentation contains detailed information. "Using SSL communication" on page 34 provides more details about SSL communication with JDK.

8. Run the random generator as root using the following command:

```
/sbin/rngd -b -r /dev/urandom -o /dev/random
```

   Note: If the operating system is upgraded to Linux 7.x/8.x/9.x, then run the following command as root:

```
ln -s /usr/lib64/libsasl2.so.3.0.0 /usr/lib64/libsasl2.so.2
```

9. Run the Documentum CM Server installation program.

   a. Run `serverSetup.bin`.

   Note: Before you install Documentum CM Server on Linux, ensure that you have completed the following tasks:

   - Install the Expect version 5.45.4 or earlier script utility.
   - Install the TCL version 8.6.8 or earlier script utility.

   The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more details.

   b. Click **Yes** when the installer displays a message stating that you are trying to upgrade the older version and asks if you want to proceed.

   c. Accept the license agreement and click **Next**.

   d. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

   e. If you select the **Enable Vault** check box, provide the following information and click **Next**:

      i. **DSIS URL**: Provide a value in the following format:

```
http://localhost:<port mentioned in application.properties>/dsis
```

      ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

> **Important**
> If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

f. Browse and specify the directory where the supported version of JDK is installed. Click **Next**.

g. Set the administrator password and specify an available listening port for the embedded application server used by Documentum CM Server and click **Next**.

- **Admin User Password**: Application server password. You must follow the password complexity rules. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about the password complexity rules.
  - If HashiCorp Vault is enabled, then the application server password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, then type the application server password.
- **Listen Port**: The port on which the application server listens for standard administration connections. A total of 20 ports, starting from the one you specify is used by the application server, and all of them must be available. The default port number is 9080. Irrespective of you accepting the default port or choosing another one, do not change this port after the initial configuration.

h. Review the installation summary and click **Install** to begin installation.

i. To open the Documentum CM Server configuration program and configure the repository, select **Configure now** and click **Done**.

10. Upgrade the connection broker.

a. Open the Documentum CM Server configuration program.

b. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

c. If you select the **Enable Vault** check box, provide the following information and click **Next**:

i. **DSIS URL**: Provide a value in the following format:

```
http://localhost:<port mentioned in application.properties>/dsis
```

ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

> **Important**
> If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make

sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

d. Select **Connection broker** and click **Next**.

e. Select **Upgrade a connection broker**.

f. Select the connection broker to upgrade from the list and click **Next**.

g. Complete the configuration, select **Perform additional configuration**, and click **Next**.

11. Upgrade the existing repository.

a. On the configuration program options page, select **Repository** and then click **Next**.

b. Select **Upgrade an existing repository**.

c. Select the repository to upgrade from the list, and click **Next**.

d. For creating new AEK key or use existing AEK key, refer to the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

e. Type the **Connection Broker Port** and **Connection Broker Host** and click **Next**.

f. Select the **Connection Mode** for the repository and click **Next**. If you select the **Secure** or **Native and Secure** options, select **Use certificate** on the next page and provide the required details.

If HashiCorp Vault is enabled, to prepare the certificate passwords, the contents of the `broker.pwd` and `server.pwd` files must be updated with the `<secret_name>/<key_name>`. For example:

In the `broker.pwd` file:

```
DOCBROKER_CERT_PASSWORD/<host name of connection broker>
```

In the `server.pwd` file:

```
DOCBASE_CERT_PASSWORD/<repository name>
```

Click **Next**.

g. Select the type of mail server, perform the tasks depending on the mail server you select, and click **Next**. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.

h. Optional Select **Enable External User Metrics Service** if you want to track the external user transactions and click **Next**.

i. Optional Select the **XML Store** check box if you want XML Store, specify the following information, and click **Next**:

- **XML Store Host**: Host name of the machine where BaseX server is installed and running.
- **XML Store Port**: Port on which BaseX server is running.

- **XML Store Administrator/Superuser password**: Password of the admin user in BaseX.
  - If HashiCorp Vault is enabled, the XML Store administrator/ superuser password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, type the XML Store administrator/superuser password.

j. Specify the data file path for BaseX and click **Next**.

k. Provide the repository owner password and click **Next**.

- If HashiCorp Vault is enabled, the repository owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the repository owner password.

l. Select **Finish configuration** and click **Next**.

12. If you upgraded from an installation using FAST full-text indexing, and selected xPlore full-text indexing, you must restart Documentum CM Server again after you complete the Documentum CM Server configuration.

13. After you complete the Documentum CM Server configuration, create a nonunique index on the `dm_sysobject.r_object_id` and `r_aspect_name` properties by using the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dm_sysobject',
attribute='r_aspect_name',use_id_col=true
```

The inclusion of the use_id_col argument set to true automatically causes Documentum CM Server to include the r_object_id column in the index.

14. If you are upgrading a repository in a distributed environment that uses a Branch Office Caching Services and asynchronous write jobs, create an index on the `dmr_content_s` (`i_parked_state`, `r_object_id`) properties. Use the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dmr_content',
attribute='i_parked_state',use_id_col=true,id_in_front=false
```

5.14.3 Post-upgrade tasks

Follow the steps provided in "Post-upgrade tasks" on page 105.

5.15 Upgrading Documentum CM Server 23.2 to 25.4 – Windows/SQL Server

The following table lists the base and upgraded versions of the Documentum CM Server, operating system, and database that are supported in this upgrade scenario:

Table 5-14: Base and upgraded OS/DB/Documentum CM Server versions

	Base version	Upgraded version
Operating System	Windows Server 2022 (64-bit)	Windows Server 2022 (64-bit)
Database	SQL Server 2022	SQL Server 2022
Documentum CM Server	64-bit Documentum CM Server 23.2	64-bit Documentum CM Server 25.4

5.15.1 Pre-upgrade tasks

1. Review the "Upgrading Documentum CM Server" on page 35.
2. Back up the repository.
3. Ensure that you apply the latest Documentum CM Server patch.
4. Optional Take a backup of all users that are part of the *Admin group*. In addition, ensure that you take the backup of the customized attribute like group_address.
5. If the repository contains customized repository formats (dm_format objects), back up the customized formats.
6. Temporarily increase the amount of rollback space available in the RDBMS. The number of rollback segments should be commensurate with the size of the repository and should be in segments of equal size. For the steps, refer to the database documentation.
7. Ensure that you have sufficient disk space on the computer hosting the database.
8. Run the Consistency Checker tool. The syntax is:

```
dmbasic -fconsistency_checker.ebs -eEntry_Point -- <repository_name>
<superuser> <password>
```

9. Fix the inconsistencies reported by the Consistency Checker tool as errors.
10. Ensure that the dm_server_config object is unlocked.
11. Optional If you are upgrading Documentum CM Server enabled with SSL communication and lockbox, perform the following tasks:
    a. Remove the key from the lockbox using the following example command format:

```
dm_crypto_create -lockbox lockbox.lb -lockboxpassphrase Password@123 -keyname
CSaek -removelockbox -output CSaek
```

b. Comment the `crypto_lockbox` section from all the `docbroker.ini` and `server.ini` files.

c. Restart the connection broker and the repository and ensure that they start properly.

12. If you want to upgrade AEK key, make sure that you update the AEK passphrase to comply with password complexity rules using the following command format:

```
dm_crypto_change_passphrase.exe -keyname <name of aek key> -passphrase <old
passsphrase> -newpassphrase <new password with complexity rules>
```

For example:

```
dm_crypto_change_passphrase.exe -keyname aek_name -passphrase Password@123 -
newpassphrase Password@1234567890
```

The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about password complexity rules.

Note: This step is valid only when upgrading to a repository where HashiCorp Vault is not enabled.

13. If you want to upgrade AEK key in a repository where HashiCorp Vault is enabled, then you must create HashiCorp Vault-based AEK keys.

OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD) contains detailed information.

5.15.2 Upgrade tasks

1. Upgrade the Windows operating system to Windows Server 2022 (64-bit).
2. Install the latest version of Microsoft Visual C++ 2013, 2019, and 2022 Redistributable (64-bit) package before upgrading a repository. This provides the correct operating system runtime libraries for the Documentum CM Server and other utilities.
3. Upgrade the database to SQL Server 2022 for Microsoft Windows with latest cumulative update.
4. Disable all jobs.

   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.

   b. Right-click the job and select **Properties**.

   c. On the **Properties** page, set the **State** to `Inactive`.

5. Shut down the repositories and connection brokers.

   a. Click **Start > Programs > Documentum > Server Manager**.

b. Select the correct Documentum CM Server and click **Stop**.

c. On the **Connection Broker** tab, select each connection broker, and then click **Stop**.

6. To shut down the application server on Windows, stop the service called Java Method Server. Ensure that the application server does not start automatically after a host restart.

   Click **Start > Control Panel > Administrative Tools > Services**, select the **Java Method Server**, and then click **Stop**.

7. Download and install the supported version of Oracle JDK/OpenJDK version from Oracle JDK/OpenJDK website. The *Oracle JDK and OpenJDK* documentation contains detailed information. "Using SSL communication" on page 34 provides more details about SSL communication with JDK.

8. Run the Documentum CM Server installation program.

   a. Run `serverSetup.exe`.

   b. Click **Yes** when the installer displays a message stating that you are trying to upgrade the older version and asks if you want to proceed.

   c. Accept the license agreement and click **Next**.

   d. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

   e. If you select the **Enable Vault** check box, provide the following information and click **Next**:

      i. **DSIS URL**: Provide a value in the following format:

      ```
      http://localhost:<port mentioned in application.properties>/dsis
      ```

      ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

      Important

      If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

   f. On Windows, provide the installation owner password and click **Next**.

      - If HashiCorp Vault is enabled, the installation owner password is retrieved from the HashiCorp Vault server.
      - If HashiCorp Vault is not enabled, type the installation owner password.

   g. Browse and specify the directory where the supported version of JDK is installed. Click **Next**.

   h. Set the administrator password and specify an available listening port for the embedded application server used by Documentum CM Server and click **Next**.

- **Admin User Password**: Application server password. You must follow the password complexity rules. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about the password complexity rules.
  - If HashiCorp Vault is enabled, then the application server password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, then type the application server password.
- **Listen Port**: The port on which the application server listens for standard administration connections. A total of 20 ports, starting from the one you specify is used by the application server, and all of them must be available. The default port number is 9080. Irrespective of you accepting the default port or choosing another one, do not change this port after the initial configuration.

i. Review the installation summary and click **Install** to begin installation.

j. To open the Documentum CM Server configuration program and configure the repository, select **Configure now** and click **Done**.

9. Upgrade the connection broker.

a. Open the Documentum CM Server configuration program.

b. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

c. If you select the **Enable Vault** check box, provide the following information and click **Next**:

i. **DSIS URL**: Provide a value in the following format:

```
http://localhost:<port mentioned in application.properties>/dsis
```

ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

> **Important**
> If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

d. Select **Connection broker** and click **Next**.

e. On Windows, provide the installation owner password and click **Next**.

- If HashiCorp Vault is enabled, the installation owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the installation owner password.

f. Select **Upgrade a connection broker**.

g. Select the connection broker to upgrade from the list and click **Next**.

h. Complete the configuration, select **Perform additional configuration**, and click **Next**.

10. Upgrade the existing repository.

a. On the configuration program options page, select **Repository** and then click **Next**.

b. Select **Upgrade an existing repository**.

c. Select the repository to upgrade from the list, and click **Next**.

d. For creating new AEK key or use existing AEK key, refer to the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

e. Type the **Connection Broker Port** and **Connection Broker Host** and click **Next**.

f. Select the **Connection Mode** for the repository and click **Next**. If you select the **Secure** or **Native and Secure** options, select **Use certificate** on the next page and provide the required details.

If HashiCorp Vault is enabled, to prepare the certificate passwords, the contents of the `broker.pwd` and `server.pwd` files must be updated with the `<secret_name>/<key_name>`. For example:

In the `broker.pwd` file:

```
DOCBROKER_CERT_PASSWORD/<host name of connection broker>
```

In the `server.pwd` file:

```
DOCBASE_CERT_PASSWORD/<repository name>
```

Click **Next**.

g. Select the type of mail server, perform the tasks depending on the mail server you select, and click **Next**. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.

h. Optional Select **Enable External User Metrics Service** if you want to track the external user transactions and click **Next**.

i. Optional Select the **XML Store** check box if you want XML Store, specify the following information, and click **Next**:

- **XML Store Host**: Host name of the machine where BaseX server is installed and running.
- **XML Store Port**: Port on which BaseX server is running.
- **XML Store Administrator/Superuser password**: Password of the admin user in BaseX.
  - If HashiCorp Vault is enabled, the XML Store administrator/ superuser password is retrieved from the HashiCorp Vault server.

- If HashiCorp Vault is not enabled, type the XML Store administrator/superuser password.

j. Specify the data file path for BaseX and click **Next**.

k. Provide the repository owner password and click **Next**.

- If HashiCorp Vault is enabled, the repository owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the repository owner password.

l. Select **Finish configuration** and click **Next**.

11. If you upgraded from an installation using FAST full-text indexing, and selected xPlore full-text indexing, you must restart Documentum CM Server again after you complete the Documentum CM Server configuration.

12. After you complete the Documentum CM Server configuration, create a nonunique index on the `dm_sysobject.r_object_id` and `r_aspect_name` properties by using the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dm_sysobject',
attribute='r_aspect_name',use_id_col=true
```

The inclusion of the use_id_col argument set to true automatically causes Documentum CM Server to include the r_object_id column in the index.

13. If you are upgrading a repository in a distributed environment that uses a Branch Office Caching Services and asynchronous write jobs, create an index on the `dmr_content_s` (`i_parked_state`, `r_object_id`) properties. Use the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dmr_content',
attribute='i_parked_state',use_id_col=true,id_in_front=false
```

5.15.3 Post-upgrade tasks

Follow the steps provided in "Post-upgrade tasks" on page 81.

5.16 Upgrading Documentum CM Server 23.4 to 25.4 – Windows/SQL Server

The following table lists the base and upgraded versions of the Documentum CM Server, operating system, and database that are supported in this upgrade scenario:

Table 5-15: Base and upgraded OS/DB/Documentum CM Server versions

	Base version	Upgraded version
Operating System	Windows Server 2022 (64-bit)	Windows Server 2025 (64-bit)
Database	SQL Server 2022	SQL Server 2022
Documentum CM Server	64-bit Documentum CM Server 23.4	64-bit Documentum CM Server 25.4

5.16.1 Pre-upgrade tasks

1. Review the "Upgrading Documentum CM Server" on page 35.
2. Back up the repository.
3. Ensure that you apply the latest Documentum CM Server patch.
4. Optional Take a backup of all users that are part of the *Admin group*. In addition, ensure that you take the backup of the customized attribute like group_address.
5. If the repository contains customized repository formats (dm_format objects), back up the customized formats.
6. Temporarily increase the amount of rollback space available in the RDBMS. The number of rollback segments should be commensurate with the size of the repository and should be in segments of equal size. For the steps, refer to the database documentation.
7. Ensure that you have sufficient disk space on the computer hosting the database.
8. Run the Consistency Checker tool. The syntax is:

   ```
   dmbasic -fconsistency_checker.ebs -eEntry_Point -- <repository_name>
   <superuser> <password>
   ```

9. Fix the inconsistencies reported by the Consistency Checker tool as errors.
10. Ensure that the dm_server_config object is unlocked.
11. Optional If you are upgrading Documentum CM Server enabled with SSL communication and lockbox, perform the following tasks:

    a. Remove the key from the lockbox using the following example command format:

    ```
    dm_crypto_create -lockbox lockbox.lb -lockboxpassphrase Password@123 -keyname
    CSaek -removelockbox -output CSaek
    ```

    b. Comment the `crypto_lockbox` section from all the `docbroker.ini` and `server.ini` files.

    c. Restart the connection broker and the repository and ensure that they start properly.

12. If you want to upgrade AEK key, make sure that you update the AEK passphrase to comply with password complexity rules using the following command format:

    ```
    dm_crypto_change_passphrase.exe -keyname <name of aek key> -passphrase <old
    passsphrase> -newpassphrase <new password with complexity rules>
    ```

    For example:

    ```
    dm_crypto_change_passphrase.exe -keyname aek_name -passphrase Password@123 -
    newpassphrase Password@1234567890
    ```

The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about password complexity rules.

Note: This step is valid only when upgrading to a repository where HashiCorp Vault is not enabled.

13. If you want to upgrade AEK key in a repository where HashiCorp Vault is enabled, then you must create HashiCorp Vault-based AEK keys.

    OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD) contains detailed information.

5.16.2 Upgrade tasks

1. Upgrade the Windows operating system to Windows Server 2025 (64-bit).
2. Install the latest version of Microsoft Visual C++ 2013, 2019, and 2022 Redistributable (64-bit) package before upgrading a repository. This provides the correct operating system runtime libraries for the Documentum CM Server and other utilities.
3. Upgrade the database to SQL Server 2022 for Microsoft Windows with latest cumulative update.
4. Disable all jobs.
   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
   b. Right-click the job and select **Properties**.
   c. On the **Properties** page, set the **State** to `Inactive`.
5. Shut down the repositories and connection brokers.
   a. Click **Start > Programs > Documentum > Server Manager**.
   b. Select the correct Documentum CM Server and click **Stop**.
   c. On the **Connection Broker** tab, select each connection broker, and then click **Stop**.
6. To shut down the application server on Windows, stop the service called Java Method Server. Ensure that the application server does not start automatically after a host restart.

   Click **Start > Control Panel > Administrative Tools > Services**, select the **Java Method Server**, and then click **Stop**.
7. Download and install the supported version of Oracle JDK/OpenJDK version from Oracle JDK/OpenJDK website. The *Oracle JDK and OpenJDK* documentation contains detailed information. "Using SSL communication" on page 34 provides more details about SSL communication with JDK.
8. Run the Documentum CM Server installation program.

a. Run `serverSetup.exe`.

b. Click **Yes** when the installer displays a message stating that you are trying to upgrade the older version and asks if you want to proceed.

c. Accept the license agreement and click **Next**.

d. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

e. If you select the **Enable Vault** check box, provide the following information and click **Next**:

   i. **DSIS URL**: Provide a value in the following format:

   ```
   http://localhost:<port mentioned in application.properties>/dsis
   ```

   ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

   Important

   If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

f. On Windows, provide the installation owner password and click **Next**.

   - If HashiCorp Vault is enabled, the installation owner password is retrieved from the HashiCorp Vault server.
   - If HashiCorp Vault is not enabled, type the installation owner password.

g. Browse and specify the directory where the supported version of JDK is installed. Click **Next**.

h. Set the administrator password and specify an available listening port for the embedded application server used by Documentum CM Server and click **Next**.

   - **Admin User Password**: Application server password. You must follow the password complexity rules. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about the password complexity rules.
     - If HashiCorp Vault is enabled, then the application server password is retrieved from the HashiCorp Vault server.
     - If HashiCorp Vault is not enabled, then type the application server password.
   - **Listen Port**: The port on which the application server listens for standard administration connections. A total of 20 ports, starting from the one you specify is used by the application server, and all of them must be available. The default port number is 9080. Irrespective of you

accepting the default port or choosing another one, do not change this port after the initial configuration.

i. Review the installation summary and click **Install** to begin installation.

j. To open the Documentum CM Server configuration program and configure the repository, select **Configure now** and click **Done**.

9. Upgrade the connection broker.

a. Open the Documentum CM Server configuration program.

b. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

c. If you select the **Enable Vault** check box, provide the following information and click **Next**:

i. **DSIS URL**: Provide a value in the following format:

```
http://localhost:<port mentioned in application.properties>/dsis
```

ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

> **Important**
> If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

d. Select **Connection broker** and click **Next**.

e. On Windows, provide the installation owner password and click **Next**.

- If HashiCorp Vault is enabled, the installation owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the installation owner password.

f. Select **Upgrade a connection broker**.

g. Select the connection broker to upgrade from the list and click **Next**.

h. Complete the configuration, select **Perform additional configuration**, and click **Next**.

10. Upgrade the existing repository.

a. On the configuration program options page, select **Repository** and then click **Next**.

b. Select **Upgrade an existing repository**.

c. Select the repository to upgrade from the list, and click **Next**.

d. For creating new AEK key or use existing AEK key, refer to the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

e. Type the **Connection Broker Port** and **Connection Broker Host** and click **Next**.

f. Select the **Connection Mode** for the repository and click **Next**. If you select the **Secure** or **Native and Secure** options, select **Use certificate** on the next page and provide the required details.

If HashiCorp Vault is enabled, to prepare the certificate passwords, the contents of the `broker.pwd` and `server.pwd` files must be updated with the `<secret_name>/<key_name>`. For example:

In the `broker.pwd` file:

```
DOCBROKER_CERT_PASSWORD/<host name of connection broker>
```

In the `server.pwd` file:

```
DOCBASE_CERT_PASSWORD/<repository name>
```

Click **Next**.

g. Select the type of mail server, perform the tasks depending on the mail server you select, and click **Next**. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.

h. Optional Select **Enable External User Metrics Service** if you want to track the external user transactions and click **Next**.

i. Optional Select the **XML Store** check box if you want XML Store, specify the following information, and click **Next**:

- **XML Store Host**: Host name of the machine where BaseX server is installed and running.
- **XML Store Port**: Port on which BaseX server is running.
- **XML Store Administrator/Superuser password**: Password of the admin user in BaseX.
  - If HashiCorp Vault is enabled, the XML Store administrator/ superuser password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, type the XML Store administrator/superuser password.

j. Specify the data file path for BaseX and click **Next**.

k. Provide the repository owner password and click **Next**.

- If HashiCorp Vault is enabled, the repository owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the repository owner password.

l. Select **Finish configuration** and click **Next**.

11. If you upgraded from an installation using FAST full-text indexing, and selected xPlore full-text indexing, you must restart Documentum CM Server again after you complete the Documentum CM Server configuration.

12. After you complete the Documentum CM Server configuration, create a nonunique index on the `dm_sysobject.r_object_id` and `r_aspect_name` properties by using the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dm_sysobject',
attribute='r_aspect_name',use_id_col=true
```

    The inclusion of the use_id_col argument set to true automatically causes Documentum CM Server to include the r_object_id column in the index.

13. If you are upgrading a repository in a distributed environment that uses a Branch Office Caching Services and asynchronous write jobs, create an index on the `dmr_content_s` (`i_parked_state`, `r_object_id`) properties. Use the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dmr_content',
attribute='i_parked_state',use_id_col=true,id_in_front=false
```

5.16.3 Post-upgrade tasks

Follow the steps provided in "Post-upgrade tasks" on page 81.

5.17 Upgrading Documentum CM Server 24.2 to 25.4 – Windows/PostgreSQL

The following table lists the base and upgraded versions of the Documentum CM Server, operating system, and database that are supported in this upgrade scenario:

Table 5-16: Base and upgraded OS/DB/Documentum CM Server versions

	Base version	Upgraded version
Operating System	Windows Server 2022 (64-bit)	Windows Server 2025 (64-bit)
Database	PostgreSQL 14	PostgreSQL 16.x
Documentum CM Server	64-bit Documentum CM Server 24.2	64-bit Documentum CM Server 25.4

5.17.1 Pre-upgrade tasks

1. Review the "Upgrading Documentum CM Server" on page 35.
2. If you are installing the xPlore indexing server, review the *OpenText Documentum xPlore Installation Guide*.
3. Back up the repository.
4. Optional Take a backup of all users that are part of the *Admin group*. In addition, ensure that you take the backup of the customized attribute like group_address.
5. If the repository contains customized repository formats (dm_format objects), back up the customized formats.

6. Ensure that you have sufficient disk space on the computer hosting the database.
7. Run the Consistency Checker tool. The syntax is:

```
dmbasic -fconsistency_checker.ebs -eEntry_Point -- <repository_name>
<superuser> <password>
```

8. Fix the inconsistencies reported by the Consistency Checker tool as errors.
9. Ensure that the dm_server_config object is unlocked.
10. If you want to upgrade AEK key, make sure that you update the AEK passphrase to comply with password complexity rules using the following command format:

```
dm_crypto_change_passphrase.exe -keyname <name of aek key> -passphrase <old
passsphrase> -newpassphrase <new password with complexity rules>
```

For example:

```
dm_crypto_change_passphrase.exe -keyname aek_name -passphrase Password@123 -
newpassphrase Password@1234567890
```

The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about password complexity rules.

Note: This step is valid only when upgrading to a repository where HashiCorp Vault is not enabled.

11. If you want to upgrade AEK key in a repository where HashiCorp Vault is enabled, then you must create HashiCorp Vault-based AEK keys.

OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD) contains detailed information.

5.17.2 Upgrade tasks

1. Upgrade the Windows operating system to Windows Server 2025 (64-bit).
2. Install the latest version of Microsoft Visual C++ 2013, 2019, and 2022 Redistributable (64-bit) package before upgrading a repository. This provides the correct operating system runtime libraries for the Documentum CM Server and other utilities.
3. Upgrade the database to PostgreSQL 16.x.
4. Disable all jobs.
   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
   b. Right-click the job and select **Properties**.
   c. On the **Properties** page, set the **State** to `Inactive`.
5. Shut down the repositories and connection brokers.

a. Click **Start > Programs > Documentum > Server Manager**.

b. Select the correct Documentum CM Server and click **Stop**.

c. On the **Connection Broker** tab, select each connection broker and click **Stop**.

6. To shut down the application server on Windows, stop the service called Java Method Server. Ensure that the application server does not start automatically after a host restart.

   Click **Start > Control Panel > Administrative Tools > Services**, select the **Java Method Server**, and click **Stop**.

7. Download and install the supported version of Oracle JDK/OpenJDK version from Oracle JDK/OpenJDK website. The *Oracle JDK and OpenJDK* documentation contains detailed information. "Using SSL communication" on page 34 provides more details about SSL communication with JDK.

8. Run the Documentum CM Server installation program.

   a. Run `serverSetup.bin`.

   Note: Before you install Documentum CM Server on Linux, ensure that you have completed the following tasks:

   - Install the Expect version 5.45.4 or earlier script utility.
   - Install the TCL version 8.6.8 or earlier script utility.

   The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more details.

   b. Click **Yes** when the installer displays a message stating that you are trying to upgrade the older version and asks if you want to proceed.

   c. Accept the license agreement and click **Next**.

   d. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

   e. If you select the **Enable Vault** check box, provide the following information and click **Next**:

      i. **DSIS URL**: Provide a value in the following format:

      ```
      http://localhost:<port mentioned in application.properties>/dsis
      ```

      ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

      Important

      If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from HashiCorp Vault. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

f. Browse and specify the directory where the supported version of JDK is installed. Click **Next**.

g. Set the administrator password and specify an available listening port for the embedded application server used by Documentum CM Server and click **Next**.

- **Admin User Password**: Application server password. You must follow the password complexity rules. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about the password complexity rules.
  - If HashiCorp Vault is enabled, then the application server password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, then type the application server password.
- **Listen Port**: The port on which the application server listens for standard administration connections. A total of 20 ports, starting from the one you specify is used by the application server, and all of them must be available. The default port number is 9080. Irrespective of you accepting the default port or choosing another one, do not change this port after the initial configuration.

h. Review the installation summary and click **Install** to begin installation.

i. To open the Documentum CM Server configuration program and configure the repository, select **Configure now** and click **Done**.

9. Upgrade the connection broker.

a. Open the Documentum CM Server configuration program.

b. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

c. If you select the **Enable Vault** check box, provide the following information and click **Next**:

i. **DSIS URL**: Provide a value in the following format:

```
http://localhost:<port mentioned in application.properties>/dsis
```

ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

> **Important**
> If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from HashiCorp Vault. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

d. Select **Connection broker** and click **Next**.

e. Select **Upgrade a connection broker**.

f. Select the connection broker to upgrade from the list and click **Next**.

g. Complete the configuration, select **Perform additional configuration**, and click **Next**.

10. Upgrade the existing repository.

a. On the configuration program options page, select **Repository** and then click **Next**.

b. Select **Upgrade an existing repository**.

c. Select the repository to upgrade from the list, and click **Next**.

d. For creating new AEK key or use existing AEK key, refer to the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

e. Type the **Connection Broker Port** and **Connection Broker Host** and click **Next**.

f. Select the **Connection Mode** for the repository and click **Next**. If you select the **Secure** or **Native and Secure** options, select **Use certificate** on the next page and provide the required details.

If HashiCorp Vault is enabled, to prepare the certificate passwords, the contents of the `broker.pwd` and `server.pwd` files must be updated with the `<secret_name>/<key_name>`. For example:

In the `broker.pwd` file:

```
DOCBROKER_CERT_PASSWORD/<host name of connection broker>
```

In the `server.pwd` file:

```
DOCBASE_CERT_PASSWORD/<repository name>
```

Click **Next**.

g. Select the type of mail server, perform the tasks depending on the mail server you select, and click **Next**. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.

h. Optional Select **Enable External User Metrics Service** if you want to track the external user transactions and click **Next**.

i. Optional Select the **XML Store** check box if you want XML Store, specify the following information, and click **Next**:

- **XML Store Host**: Host name of the machine where BaseX server is installed and running.
- **XML Store Port**: Port on which BaseX server is running.
- **XML Store Administrator/Superuser password**: Password of the admin user in BaseX.
  - If HashiCorp Vault is enabled, the XML Store administrator/ superuser password is retrieved from the HashiCorp Vault server.

– If HashiCorp Vault is not enabled, type the XML Store administrator/superuser password.

j. Specify the data file path for BaseX and click **Next**.

k. Provide the repository owner password and click **Next**.

- If HashiCorp Vault is enabled, the repository owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the repository owner password.

l. Select **Finish configuration** and click **Next**.

11. If you upgraded from an installation using FAST full-text indexing, and selected xPlore full-text indexing, you must restart Documentum CM Server again after you complete the Documentum CM Server configuration.

12. After you complete the Documentum CM Server configuration, create a nonunique index on the `dm_sysobject.r_object_id` and `r_aspect_name` properties by using the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dm_sysobject',
attribute='r_aspect_name',use_id_col=true
```

The inclusion of the use_id_col argument set to true automatically causes Documentum CM Server to include the r_object_id column in the index.

13. If you are upgrading a repository in a distributed environment that uses a Branch Office Caching Services and asynchronous write jobs, create an index on the `dmr_content_s` (`i_parked_state`, `r_object_id`) properties. Use the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dmr_content',
attribute='i_parked_state',use_id_col=true,id_in_front=false
```

5.17.3 Post-upgrade tasks

Follow the steps provided in "Post-upgrade tasks" on page 81.

5.18 Upgrading Documentum CM Server 24.4 to 25.4 – Windows/Oracle

The following table lists the base and upgraded versions of the Documentum CM Server, operating system, and database that are supported in this upgrade scenario:

Table 5-17: Base and upgraded OS/DB/Documentum CM Server versions

	Base version	Upgraded version
Operating System	Windows Server 2022 (64-bit)	Windows Server 2022 (64-bit)
Database	Oracle 19c	Oracle 19c
Documentum CM Server	64-bit Documentum CM Server 24.4	64-bit Documentum CM Server 25.4

5.18.1 Pre-upgrade tasks

Follow the steps provided in "Pre-upgrade tasks" on page 118.

5.18.2 Upgrade tasks

1. Install the latest version of Microsoft Visual C++ 2013, 2019, and 2022 Redistributable (64-bit) package before upgrading a repository. This provides the correct operating system runtime libraries for the Documentum CM Server and other utilities.
2. After you upgrade the database, create an `ORACLE_HOME` environment variable in Windows that points to the location of the 64-bit `tnsnames.ora` file. The entries from the 32-bit `tnsnames.ora` file have to be copied into the 64-bit `tnsnames.ora` file.
3. Disable all jobs.
   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
   b. Right-click the job and select **Properties**.
   c. On the **Properties** page, set the **State** to `Inactive`.
4. Shut down the repositories and connection brokers.
   a. Click **Start > Programs > Documentum > Server Manager**.
   b. Select the correct Documentum CM Server and click **Stop**.
   c. On the **Connection Broker** tab, select each connection broker, and then click **Stop**.
5. To shut down the application server on Windows, stop the service called Java Method Server. Ensure that the application server does not start automatically after a host restart.

   Click **Start > Control Panel > Administrative Tools > Services**, select the **Java Method Server**, and then click **Stop**.
6. During the upgrade from 32-bit to 64-bit, Documentum CM Server, you cannot upgrade the authentication plug-ins that you have installed. You need to replace the 32-bit authentication plug-ins with the 64-bit plug-ins. You can find the plug-ins in the `%DM_HOME%\install\external_apps\authplugins` folder.
7. Download and install the supported version of Oracle JDK/OpenJDK version from Oracle JDK/OpenJDK website. The *Oracle JDK and OpenJDK* documentation contains detailed information. "Using SSL communication" on page 34 provides more details about SSL communication with JDK.
8. Run the Documentum CM Server installation program.
   a. Run `serverSetup.exe`.

b. Click **Yes** when the installer displays a message stating that you are trying to upgrade the older version and asks if you want to proceed.

c. Accept the license agreement and click **Next**.

d. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

e. If you select the **Enable Vault** check box, provide the following information and click **Next**:

   i. **DSIS URL**: Provide a value in the following format:

   ```
   http://localhost:<port mentioned in application.properties>/dsis
   ```

   ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

> **Important**
> If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

f. On Windows, provide the installation owner password and click **Next**.

- If HashiCorp Vault is enabled, the installation owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the installation owner password.

g. Browse and specify the directory where the supported version of JDK is installed. Click **Next**.

h. Set the administrator password and specify an available listening port for the embedded application server used by Documentum CM Server and click **Next**.

- **Admin User Password**: Application server password. You must follow the password complexity rules. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about the password complexity rules.
  - If HashiCorp Vault is enabled, then the application server password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, then type the application server password.
- **Listen Port**: The port on which the application server listens for standard administration connections. A total of 20 ports, starting from the one you specify is used by the application server, and all of them must be available. The default port number is 9080. Irrespective of you accepting the default port or choosing another one, do not change this port after the initial configuration.

i. Review the installation summary and click **Install** to begin installation.

j. To open the Documentum CM Server configuration program and configure the repository, select **Configure now** and click **Done**.

9. Upgrade the connection broker.

a. Open the Documentum CM Server configuration program.

b. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

c. If you select the **Enable Vault** check box, provide the following information and click **Next**:

i. **DSIS URL**: Provide a value in the following format:

```
http://localhost:<port mentioned in application.properties>/dsis
```

ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

> **Important**
> If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

d. Select **Connection broker** and click **Next**.

e. On Windows, provide the installation owner password and click **Next**.

- If HashiCorp Vault is enabled, the installation owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the installation owner password.

f. Select **Upgrade a connection broker**.

g. Select the connection broker to upgrade from the list and click **Next**.

h. Complete the configuration, select **Perform additional configuration**, and click **Next**.

10. Upgrade the existing repository.

a. On the configuration program options page, select **Repository** and then click **Next**.

b. Select **Upgrade an existing repository**.

c. Select the repository to upgrade from the list, and click **Next**.

d. You can choose if you want to upgrade AEK key or continue with the existing AEK key. Take a backup of the AEK key. For creating new AEK key, refer to the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

e. Type the **Connection Broker Port** and **Connection Broker Host** and click **Next**.

f. Select the **Connection Mode** for the repository and click **Next**. If you select the **Secure** or **Native and Secure** options, select **Use certificate** on the next page and provide the required details.

If HashiCorp Vault is enabled, to prepare the certificate passwords, the contents of the `broker.pwd` and `server.pwd` files must be updated with the `<secret_name>/<key_name>`. For example:

In the `broker.pwd` file:

```
DOCBROKER_CERT_PASSWORD/<host name of connection broker>
```

In the `server.pwd` file:

```
DOCBASE_CERT_PASSWORD/<repository name>
```

Click **Next**.

g. Select the type of mail server, perform the tasks depending on the mail server you select, and click **Next**. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.

h. Optional Select **Enable External User Metrics Service** if you want to track the external user transactions and click **Next**.

i. Optional Select the **XML Store** check box if you want XML Store, specify the following information, and click **Next**:

- **XML Store Host**: Host name of the machine where BaseX server is installed and running.
- **XML Store Port**: Port on which BaseX server is running.
- **XML Store Administrator/Superuser password**: Password of the admin user in BaseX.
  - If HashiCorp Vault is enabled, the XML Store administrator/superuser password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, type the XML Store administrator/superuser password.

j. Specify the data file path for BaseX and click **Next**.

k. Provide the repository owner password and click **Next**.

- If HashiCorp Vault is enabled, the repository owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the repository owner password.

l. Select **Finish configuration** and click **Next**.

11. If you upgraded from an installation using FAST full-text indexing, and selected xPlore full-text indexing, you must restart Documentum CM Server again after you complete the Documentum CM Server configuration.

12. After you complete the Documentum CM Server configuration, create a nonunique index on the `dm_sysobject.r_object_id` and `r_aspect_name` properties by using the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dm_sysobject',
attribute='r_aspect_name',use_id_col=true
```

The inclusion of the use_id_col argument set to true automatically causes Documentum CM Server to include the r_object_id column in the index.

13. If you are upgrading a repository in a distributed environment that uses a Branch Office Caching Services and asynchronous write jobs, create an index on the `dmr_content_s` (`i_parked_state`, `r_object_id`) properties. Use the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dmr_content',
attribute='i_parked_state',use_id_col=true,id_in_front=false
```

5.18.3 Post-upgrade tasks

Follow the steps provided in "Post-upgrade tasks" on page 81.

5.19 Upgrading Documentum CM Server 25.2 to 25.4 – Windows/Oracle

The following table lists the base and upgraded versions of the Documentum CM Server, operating system, and database that are supported in this upgrade scenario:

Table 5-18: Base and upgraded OS/DB/Documentum CM Server versions

	Base version	Upgraded version
Operating System	Windows Server 2022 (64-bit)	Windows Server 2025 (64-bit)
Database	Oracle 19c	Oracle 19c
Documentum CM Server	64-bit Documentum CM Server 25.2	64-bit Documentum CM Server 25.4

5.19.1 Pre-upgrade tasks

Follow the steps provided in "Pre-upgrade tasks" on page 118.

5.19.2 Upgrade tasks

1. Upgrade the Windows operating system to Windows Server 2025 (64-bit).
2. Install the latest version of Microsoft Visual C++ 2013, 2019, and 2022 Redistributable (64-bit) package before upgrading a repository. This provides the correct operating system runtime libraries for the Documentum CM Server and other utilities.
3. After you upgrade the database, create an `ORACLE_HOME` environment variable in Windows that points to the location of the 64-bit `tnsnames.ora` file. The entries from the 32-bit `tnsnames.ora` file have to be copied into the 64-bit `tnsnames.ora` file.

4. Disable all jobs.

   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
   b. Right-click the job and select **Properties**.
   c. On the **Properties** page, set the **State** to `Inactive`.

5. Shut down the repositories and connection brokers.

   a. Click **Start > Programs > Documentum > Server Manager**.
   b. Select the correct Documentum CM Server and click **Stop**.
   c. On the **Connection Broker** tab, select each connection broker, and then click **Stop**.

6. To shut down the application server on Windows, stop the service called Java Method Server. Ensure that the application server does not start automatically after a host restart.

   Click **Start > Control Panel > Administrative Tools > Services**, select the **Java Method Server**, and then click **Stop**.

7. During the upgrade from 32-bit to 64-bit, Documentum CM Server, you cannot upgrade the authentication plug-ins that you have installed. You need to replace the 32-bit authentication plug-ins with the 64-bit plug-ins. You can find the plug-ins in the `%DM_HOME%\install\external_apps\authplugins` folder.

8. Download and install the supported version of Oracle JDK/OpenJDK version from Oracle JDK/OpenJDK website. The *Oracle JDK and OpenJDK* documentation contains detailed information. "Using SSL communication" on page 34 provides more details about SSL communication with JDK.

9. Run the Documentum CM Server installation program.

   a. Run `serverSetup.exe`.
   b. Click **Yes** when the installer displays a message stating that you are trying to upgrade the older version and asks if you want to proceed.
   c. Accept the license agreement and click **Next**.
   d. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.
   e. If you select the **Enable Vault** check box, provide the following information and click **Next**:

      i. **DSIS URL**: Provide a value in the following format:

      ```
      http://localhost:<port mentioned in application.properties>/dsis
      ```

      ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

      Important

      If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make

sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

f. On Windows, provide the installation owner password and click **Next**.

- If HashiCorp Vault is enabled, the installation owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the installation owner password.

g. Browse and specify the directory where the supported version of JDK is installed. Click **Next**.

h. Set the administrator password and specify an available listening port for the embedded application server used by Documentum CM Server and click **Next**.

- **Admin User Password**: Application server password. You must follow the password complexity rules. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information about the password complexity rules.
  - If HashiCorp Vault is enabled, then the application server password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, then type the application server password.
- **Listen Port**: The port on which the application server listens for standard administration connections. A total of 20 ports, starting from the one you specify is used by the application server, and all of them must be available. The default port number is 9080. Irrespective of you accepting the default port or choosing another one, do not change this port after the initial configuration.

i. Review the installation summary and click **Install** to begin installation.

j. To open the Documentum CM Server configuration program and configure the repository, select **Configure now** and click **Done**.

10. Upgrade the connection broker.

a. Open the Documentum CM Server configuration program.

b. If you want to configure HashiCorp Vault secrets, on the **Vault configuration** page, select the **Enable Vault** check box.

c. If you select the **Enable Vault** check box, provide the following information and click **Next**:

i. **DSIS URL**: Provide a value in the following format:

```
http://localhost:<port mentioned in application.properties>/dsis
```

ii. **DSIS Token**: Provide the `dsis.dctm.token` token value.

> **Important**
> If HashiCorp Vault is enabled, the installer retrieves all the password information automatically from the HashiCorp Vault server. Make sure that you have stored all the required secrets as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

d. Select **Connection broker** and click **Next**.

e. On Windows, provide the installation owner password and click **Next**.

- If HashiCorp Vault is enabled, the installation owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the installation owner password.

f. Select **Upgrade a connection broker**.

g. Select the connection broker to upgrade from the list and click **Next**.

h. Complete the configuration, select **Perform additional configuration**, and click **Next**.

11. Upgrade the existing repository.

a. On the configuration program options page, select **Repository** and then click **Next**.

b. Select **Upgrade an existing repository**.

c. Select the repository to upgrade from the list, and click **Next**.

d. You can choose if you want to upgrade AEK key or continue with the existing AEK key. Take a backup of the AEK key. For creating new AEK key, refer to the *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

e. Type the **Connection Broker Port** and **Connection Broker Host** and click **Next**.

f. Select the **Connection Mode** for the repository and click **Next**. If you select the **Secure** or **Native and Secure** options, select **Use certificate** on the next page and provide the required details.

If HashiCorp Vault is enabled, to prepare the certificate passwords, the contents of the `broker.pwd` and `server.pwd` files must be updated with the `<secret_name>/<key_name>`. For example:

In the `broker.pwd` file:

```
DOCBROKER_CERT_PASSWORD/<host name of connection broker>
```

In the `server.pwd` file:

```
DOCBASE_CERT_PASSWORD/<repository name>
```

Click **Next**.

g. Select the type of mail server, perform the tasks depending on the mail server you select, and click **Next**. *OpenText Documentum Content*

Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD) contains detailed information.

h. Optional Select **Enable External User Metrics Service** if you want to track the external user transactions and click **Next**.

i. Optional Select the **XML Store** check box if you want XML Store, specify the following information, and click **Next**:

- **XML Store Host**: Host name of the machine where BaseX server is installed and running.
- **XML Store Port**: Port on which BaseX server is running.
- **XML Store Administrator/Superuser password**: Password of the admin user in BaseX.
  - If HashiCorp Vault is enabled, the XML Store administrator/superuser password is retrieved from the HashiCorp Vault server.
  - If HashiCorp Vault is not enabled, type the XML Store administrator/superuser password.

j. Specify the data file path for BaseX and click **Next**.

k. Provide the repository owner password and click **Next**.

- If HashiCorp Vault is enabled, the repository owner password is retrieved from the HashiCorp Vault server.
- If HashiCorp Vault is not enabled, type the repository owner password.

l. Select **Finish configuration** and click **Next**.

12. If you upgraded from an installation using FAST full-text indexing, and selected xPlore full-text indexing, you must restart Documentum CM Server again after you complete the Documentum CM Server configuration.

13. After you complete the Documentum CM Server configuration, create a nonunique index on the `dm_sysobject.r_object_id` and `r_aspect_name` properties by using the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dm_sysobject',
attribute='r_aspect_name',use_id_col=true
```

The inclusion of the use_id_col argument set to true automatically causes Documentum CM Server to include the r_object_id column in the index.

14. If you are upgrading a repository in a distributed environment that uses a Branch Office Caching Services and asynchronous write jobs, create an index on the `dmr_content_s` (`i_parked_state`, `r_object_id`) properties. Use the following `MAKE_INDEX` command:

```
EXECUTE make_index WITH type_name='dmr_content',
attribute='i_parked_state',use_id_col=true,id_in_front=false
```

5.19.3 Post-upgrade tasks

Follow the steps provided in "Post-upgrade tasks" on page 81.

5.20 Upgrading Documentum CM Server 22.4 to 25.4 – Linux/Oracle using silent installer

The following table lists the base and upgraded versions of the Documentum CM Server, operating system, and database that are supported in this upgrade scenario:

Table 5-19: Base and upgraded OS/DB/Documentum CM Server versions

	Base version	Upgraded version
Operating System	Red Hat Enterprise Linux 8.6 (64-bit)	Red Hat Enterprise Linux 8.10 (64-bit)
Database	Oracle 19c	Oracle 23ai
Documentum CM Server	64-bit Documentum CM Server 22.4	64-bit Documentum CM Server 25.4

5.20.1 Pre-upgrade tasks

Follow the steps in "Pre-upgrade tasks" on page 89.

5.20.2 Upgrade tasks

1. Upgrade the Linux operating system to Red Hat Enterprise Linux 8.10 (64-bit).
2. Upgrade the database to Oracle 23ai.
3. Disable all jobs.
   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
   b. Right-click the job and select **Properties**.
   c. On the **Properties** page, set the **State** to `Inactive`.
4. Shut down the repositories and connection brokers.
   a. For each repository, run the `dm_shutdown_repository` script, where repository is the name of the Documentum CM Server to be stopped.
   b. Stop each connection broker using the `dm_stop_docbroker` utility on the command line:

```
% dm_stop_docbroker [-Ppassword][-B[batch]] [-Nport_number][-Sservice_name]
```

5. To shut down the application server on Linux, stop the service called Java Method Server. Ensure that the application server does not start automatically after a host restart.

Run the script `$DM_JMS_HOME/bin/stopMethodServer.sh`.

6. Run the random generator as root using the following command:

```
/sbin/rngd -b -r /dev/urandom -o /dev/random
```

Note: If the operating system is upgraded to Linux 7.x/8.x/9.x, then run the following command as root:

```
ln -s /usr/lib64/libsasl2.so.3.0.0 /usr/lib64/libsasl2.so.2
```

7. Run the Documentum CM Server installation program using the following command:

```
serverSetup.bin -f <Path of the Silent installer property file name>/<Silent
installer property file name>
```

Note: Before you install Documentum CM Server on Linux, ensure that you have completed the following tasks:

- Install the Expect version 5.45.4 or earlier script utility.
- Install the TCL version 8.6.8 or earlier script utility.

The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides more details.

8. Optional To enable the HashiCorp Vault secrets, add the following parameters in the silent installer property file:

```
IS_VAULT_ENABLED=true
DSIS_URL=http://localhost:8200/dsis
DSIS_TOKEN=<DSIS token value>
```

The preceding list of parameters must be added in all the silent configuration files to configure with HashiCorp Vault.

a. Store all the passwords in the HashiCorp Vault server. For more information about storing all the passwords in the HashiCorp Vault server, see *HashiCorp* documentation.
b. Configure the silent installer property file and replace all password with secret ID as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.
c. If you want to enable certificate-based SSL communication, prepare the certificate passwords. If HashiCorp Vault is enabled, the contents of the `broker.pwd` and `server.pwd` files must be updated with the `<secret_name>/<key_name>`. For example:

   In the `broker.pwd` file:

   ```
   DOCBROKER_CERT_PASSWORD/<host name of connection broker>
   ```

   In the `server.pwd` file:

   ```
   DOCBASE_CERT_PASSWORD/<repository name>
   ```

9. Run the following command to upgrade the connection broker and the existing repository:

```
dm_launch_server_config_program.sh -f <Path of the Silent installer property file
name>/<Silent installer property file name>
```

a. In the silent installer property file available at `$DM_HOME/install/silent/templates` set the following entries and provide relevant information to upgrade the connection broker:

```
#### CONFIGING DOC BROKER
SERVER.CONFIGURATOR.BROKER=TRUE
SERVER.DOCBROKER_ACTION=UPGRADE
```

b. In the silent installer property file available at `$DM_HOME/install/silent/templates` set the following entries and provide relevant information to upgrade the existing repository:

```
####CONFIG DOCBASE
SERVER.CONFIGURATOR.REPOSITORY=TRUE
SERVER.DOCBASE_ACTION=UPGRADE
```

5.20.3 Post-upgrade tasks

1. Manually run `dm_root_task` as root.
2. Enable all the disabled jobs.
   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
   b. For each of the previously disabled jobs, right-click the job and select **Properties**.
   c. On the **Properties** page, set the **State** option to `Active`.
3. Set the JAVA_HOME and PATH environment variables to the JAVA_LINK directory after you complete the upgrade.
4. Optional Run `dm_filestore_unique.class` in `$DM_HOME/install/tools` to create a filestore lock file after upgrade. Processing result (success or failure) can be found in the log file.
5. After upgrade, ensure that you add the backed up list of users to the Admin group. In addition, ensure that you manually update the backed up customized attribute. Admin group is recreated as part of the upgrade process, which dissolves all group memberships for `admingroup`. Before the upgrade process, the administrator must document the groups which contain `admingroup` as a member. Similarly, the administrator must document any changes made to the `admingroup` itself. Recreation of memberships must be reapplied after completing the upgrade process.
6. After the upgrade is complete, perform the following verifications:
   a. Check whether the `<Docbroker>.log` file in the `<Documentum_Home>/dba/log/` folder contains any warning messages.
   b. Check whether the `<Docbase>.log` file in the `<Documentum_Home>/dba/log/` folder contain any exceptions or errors.

c. Check for error messages in the `%DM_JMS_HOME%/logs/catalina<timestamp>.log` file.

d. To check the OpenText Documentum CM version, in the command prompt, run the following command:

```
documentum -version
```

e. To check the Foundation Java API version, ensure that the JRE bin path is set in the PATH variable, and then in the command prompt, run the following command:

```
java DfShowVersion
```

f. You can also check the OpenText Documentum CM version mentioned in the repository and connection broker log files.

7. Enable the FIPS settings as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

8. Review the "Post-upgrade tasks" on page 59 for other post-upgrade tasks that you might need to perform.

5.21 Upgrading Documentum CM Server 23.2 to 25.4 – Windows/SQL Server using silent installer

The following table lists the base and upgraded versions of the Documentum CM Server, operating system, and database that are supported in this upgrade scenario:

Table 5-20: Base and upgraded OS/DB/Documentum CM Server versions

	Base version	Upgraded version
Operating System	Windows Server 2019 (64-bit)	Windows Server 2022 (64-bit)
Database	SQL Server 2019	SQL Server 2022
Documentum CM Server	64-bit Documentum CM Server 23.2	64-bit Documentum CM Server 25.4

5.21.1 Pre-upgrade tasks

1. Review the "Upgrading Documentum CM Server" on page 35.

2. Back up the repository.

3. Ensure that you apply the latest Documentum CM Server patch.

4. Optional Take a backup of all users that are part of the *Admin group*. In addition, ensure that you take the backup of the customized attribute like group_address.

5. If the repository contains customized repository formats (dm_format objects), back up the customized formats.

6. Temporarily increase the amount of rollback space available in the RDBMS. The number of rollback segments should be commensurate with the size of the

repository and should be in segments of equal size. For the steps, refer to the database documentation.

7. Ensure that you have sufficient disk space on the computer hosting the database.
8. Run the Consistency Checker tool. The syntax is:

```
dmbasic -fconsistency_checker.ebs -eEntry_Point -- <repository_name>
<superuser> <password>
```

9. Fix the inconsistencies reported by the Consistency Checker tool as errors.
10. Ensure that the dm_server_config object is unlocked.

5.21.2 Upgrade tasks

1. Upgrade the Windows operating system to Windows Server 2022 (64-bit).
2. Install the latest version of Microsoft Visual C++ 2013, 2019, and 2022 Redistributable (64-bit) package before upgrading a repository. This provides the correct operating system runtime libraries for the Documentum CM Server and other utilities.
3. Upgrade the database to SQL Server 2022.
4. Disable all jobs.
   a. In Documentum Administrator, go to **Administrator > Job Management > Jobs**.
   b. Right-click the job and select **Properties**.
   c. On the **Properties** page, set the **State** to `Inactive`.
5. Shut down the repositories and connection brokers.
   a. Click **Start > Programs > Documentum > Server Manager**.
   b. Select the correct Documentum CM Server and click **Stop**.
   c. On the **Connection Broker** tab, select each connection broker, and then click **Stop**.
6. To shut down the application server on Windows, stop the service called Java Method Server. Ensure that the application server does not start automatically after a host restart.

   Click **Start > Control Panel > Administrative Tools > Services**, select the **Java Method Server**, and then click **Stop**.
7. Run the Documentum CM Server installation program using the following command:

```
serverSetup.exe -f C:\silent\Windows\<Silent installer property file name>
```

8. Optional To enable the HashiCorp Vault secrets, add the following parameters in the silent installer property file:

```
IS_VAULT_ENABLED=true
DSIS_URL=http://localhost:8200/dsis
DSIS_TOKEN=<DSIS token value>
```

The preceding list of parameters must be added in all the silent configuration files to configure with HashiCorp Vault.

9. If you want to enable certificate-based SSL communication, prepare the certificate passwords. If HashiCorp Vault is enabled, the contents of the `broker.pwd` and `server.pwd` files must be updated with the `<secret_name>/<key_name>`. For example:

   In the `broker.pwd` file:

   ```
   DOCBROKER_CERT_PASSWORD/<host name of connection broker>
   ```

   In the `server.pwd` file:

   ```
   DOCBASE_CERT_PASSWORD/<repository name>
   ```

10. Run the following command to upgrade the connection broker and the existing repository:

    ```
    Server_Configuration_Program.exe -f %DM_HOME%\install\silent\templates
    \<Silent installer property file name>
    ```

    a. In the silent installer property file available at `%DM_HOME%/install/silent/templates` set the following entries and provide relevant information to upgrade the connection broker:

    ```
    #### CONFIGING DOC BROKER
    SERVER.CONFIGURATOR.BROKER=TRUE
    SERVER.DOCBROKER_ACTION=UPGRADE
    ```

    b. In the silent installer property file available at `%DM_HOME%/install/silent/templates` set the following entries and provide relevant information to upgrade the existing repository:

    ```
    ####CONFIG DOCBASE
    SERVER.CONFIGURATOR.REPOSITORY=TRUE
    SERVER.DOCBASE_ACTION=UPGRADE
    ```

    c. Store all the passwords in the HashiCorp Vault server. For more information about storing all the passwords in the HashiCorp Vault server, see *HashiCorp* documentation.

    d. Configure the silent installer property file and replace all password with secret ID as described in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

5.21.3 Post-upgrade tasks

Follow the steps provided in “Post-upgrade tasks” on page 81.

Chapter 6

Migrating Documentum CM Server

Installing a new instance of Documentum CM Server 25.4, and migrating data from a previous version on a separate host, requires a procedure different from an upgrade.

This documentation addresses any variation from the basic scenario to known issues surrounding the configuration of your Documentum CM Server 25.4.

6.1 Understanding the migration process

Documentum CM Server migration involves three phases:

- Migrating the 32-bit Documentum CM Server to the environment running a 64-bit operating system.
- Configuring the Documentum CM Server to use the existing repository.
- Upgrading the 32-bit Documentum CM Server and repository to 64-bit Documentum CM Server 25.4.

To understand the migration process, consider the following scenario as a typical deployment of a pre-25.4 32-bit Documentum CM Server in your environment.

Host 1 is running a 32-bit operating system on which a 32-bit pre-25.4 Documentum CM Server is installed. *Host 2* is the 64-bit database server running on a 64-bit operating system. In case you have a 32-bit database server, you must upgrade it to 64-bit. The 32-bit database client libraries are installed on *Host 1* and are configured to point to the database server on *Host 2*. The following diagram illustrates the described environment.

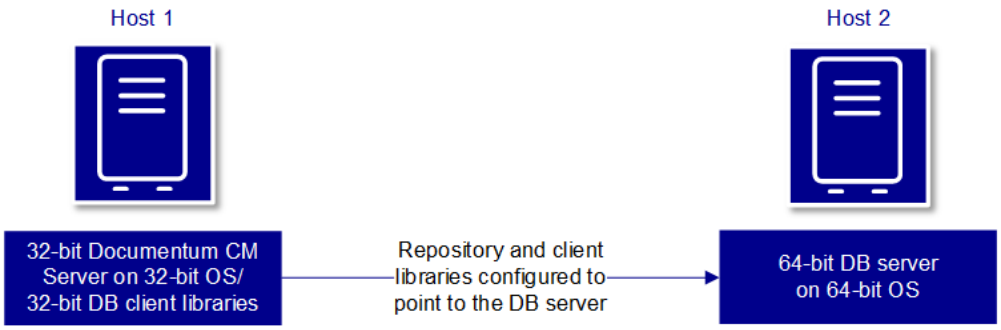


Figure 6-1: Pre-25.4 32-bit Documentum CM Server environment

You want to upgrade the 32-bit pre-25.4 Documentum CM Server on 32-bit operating system to 64-bit Documentum CM Server 25.4. Since Documentum CM

Server 25.4 requires a 64-bit operating system to run on and because no direct upgrade of a 32-bit operating system to its 64-bit version is supported, a migration of the repository is required before you can upgrade.

To migrate the repository, create another system, *Host 3*, which runs a 64-bit operating system that is compatible with the Documentum CM Server on *Host 1*. The 32-bit database client libraries are also installed on Host 3 and configured to point to *Host 2* . Install the same 32-bit Documentum CM Server that is running on *Host 1* on *Host 3*. Perform a migration of the repository filestores and content from *Host 1* to *Host 3*.

After completing all the migration tasks, configure the Documentum CM Server to use the existing repository. Upgrade the operating system on *Host 3* to the 64-bit supported version for Documentum CM Server 25.4, as specified in the product *Release Notes*. Upgrade the database on *Host 2* to the supported version. Upgrade the database client libraries to the supported 64-bit version. Finally, upgrade the 32-bit Documentum CM Server and repository to 64-bit Documentum CM Server 25.4.

The following diagram illustrates the entire migration process.

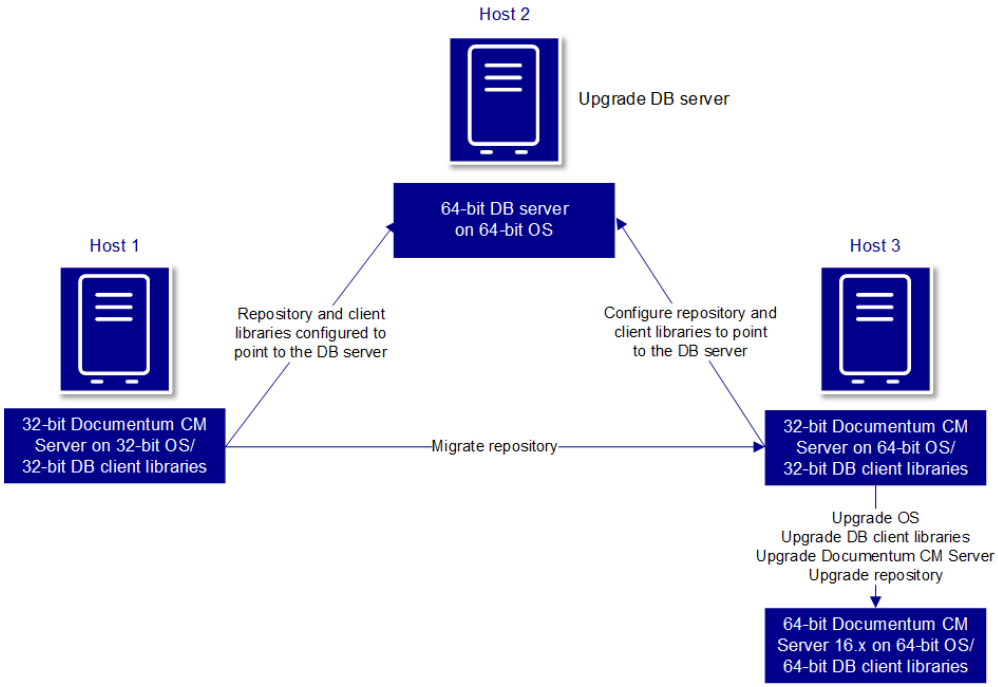


Figure 6-2: Migration process

6.2 Migration checklist

Perform the following tasks for migrating Documentum CM Server.

Table 6-1: Migration checklist

Step	Documentation
1. Prepare a plan for your migration.	See "Planning a migration" on page 188.
2. Back up your repository.	Several third-party tools are available for backup.
3. Clean up your repository.	The *OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD)* provides more information.
4. Run the Consistency Checker utility.	The "Upgrading the Documentum CM Server software" on page 44 provides the steps.
5. Fix any errors identified by the Consistency Checker.	
6. Back up your cleaned, consistent repository.	Several third-party tools are available for backup.

7. Ensure that filestore_01 is online.	You can check this two ways:
	1. Using Documentum Administrator, go to the Storage node and verify that filestore_01 shows as online.
	2. Dump the filestore and check the `r_status` attribute.
	`API>retrieve,c,dm_filestore where name='filestore_01'`
	`API>dump,c,l`
	Valid values are: 0, for on-line; 1, for off-line; 2, for read-only.

8. Install the 32-bit pre-21.1 Documentum CM Server on the target host.	The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides the installation steps.
9. Migrate the repository.	See "Migration methods" on page 189.
10. Configure Documentum CM Server to use your existing repository.	The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides the steps.
11. Upgrade Documentum CM Server and repository to 25.4.	"Upgrading the Documentum CM Server software" on page 44 provides the upgrade steps.

6.3 Planning a migration

Before you create the repository copy, complete these tasks and note any appropriate values in the Value column:

Table 6-2: Premigration tasks

Task	Resource	Value
Decide whether to copy the content files.		
Obtain the repository name.	Consult the repository administrator.	repository name: _____
Obtain the repository ID from the `server.ini` file.	Consult the repository administrator.	repository ID: _____
Obtain the repository owner's name and password.	Consult the repository administrator.	repository owner: _____
Create a database instance separate from the database instance used by the production repository.	Consult the DBA.	
Obtain connection information for the alternative database instance.	Consult the DBA and database documentation	connection: _____
Identify a target host on which to create the repository copy.		target host: _____
Obtain the system or administrator username and password for the database.	Consult the DBA.	admin user name: _____
Note the drive on which the production repository resides.		drive: _____
Decide whether to create the copy on the equivalent drive.		
Decide whether to create the copy on a drive equivalent to the drive on which the production repository resides. If the copy is on a different drive, there are additional steps you must perform.		

6.4 Migration methods

When migration a repository, you can use the following two methods depending on the type of environment:

- Migrating a repository
- Copying a repository

If the target operating system supports upgrade from source operating system, use the *Copying a repository* method. For example, Documentum CM Server 7.0 on 64-bit Windows Server 2008 R2 to Documentum CM Server 25.4 on 64-bit Windows Server 2016.

If the target operating system does not support upgrade, use the *Migrating a repository* method. For example, Documentum CM Server 6.7 SP2 on 32-bit Windows Server 2008 to Documentum CM Server 25.4 on 64-bit Windows Server 2016.

In the instructions that follow, the target repository host is called the *target host*. The source repository is called the *production repository*.

Caution

The instructions that follow assume that the production repository is running on the network while the target host is tested. However, shut down the production repository or take it off the network while you test the target host. Conflicts and data corruption can result from having two repositories on the network with the same name and repository ID.

6.4.1 Method 1: Migrating a repository

1. On the target host, install the 64-bit version of the operating system and the 32-bit version of the database client libraries.
2. Create a new Documentum CM Server installation and repository (the repository copy) of the same version number as the production repository. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides the installation steps.
3. Copy `$DOCUMENTUM/dba/secure/aek.key` and `$DOCUMENTUM/data` from the production repository host to the same locations on the target host.
4. Create a new connection broker on the target host using the Documentum CM Server configuration program. From `$DM_HOME/install`, double-click `Server_Configuration_Program.exe` to run the Documentum CM Server configuration program.
5. Configure the repository.
   - When you create the new repository, ensure that you use the same repository name, repository ID, and repository owner name and password as the production repository.

- Ensure that you use the same database instance used by the production repository. In the installer, ensure that you select the option to use an existing database user account.
- Copy the `*.cnt` files from the original host to the repository copy host for Federation and replication jobs to work.

6. Copy the `$DOCUMENTUM/dba/config/<docbase_name>/dbpasswd.txt` file from production repository host to the same location on the target host after providing the XML Store details.
7. Ensure that the repository configuration completes successfully.
8. Retrieve all the dm_jms_config objects from the repository copy and verify that the `base_uri` attribute and `projection_targets` attribute are set correctly.
   a. Start IDQL and connect to the repository as the installation owner.
   b. Run the following command to get a list of all dm_jms_config objects:
   ```
   select * from dm_jms_config
   ```
   c. Run the following command to change each projection target:
   ```
   update dm_jms_config objects set projection_targets[x]='new_target'
   where r_object_id='object_id'
   ```
   d. Run the following command to change each base URI:
   ```
   update dm_jms_config objects set base_uri[x]='new_base_uri'
   where r_object_id='object_id'
   ```
9. If you are testing the migration of a Web content management repository, modify the user objects to reflect the new authentication domain.
   a. Start IDQL and connect to the repository as the installation owner.
   b. Run the following commands:
   ```
   update dm_user objects
   set user_login_domain ='new_machine_name' where
   user_login_domain ='old_machine_name'
   ```
   c. Disconnect from the repository and exit IDQL.
10. If Documentum CM Server and content files of the copy reside on a drive different from the drive used by the production repository, use IDQL to update the `file_system_path` attribute of the dm_location and dm_mount_point objects to the new location:
    ```
    update dm_location objects
    set file_system_path='newpath' where file_system_path='old path'
    update dm_mount_point objects
    set file_system_path='newpath' where file_system_path='old path'
    ```
11. Restart Documentum CM Server.

6.4.2 Method 2: Copying a repository

1. Shut down the production repository.
2. On the target host, create a new Documentum CM Server installation and repository (the repository copy) of the same version number as the production repository. The *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* provides the installation steps.

   - When you create the repository copy, ensure that you use the same repository name, repository ID, and repository owner name and password as the production repository. In addition, the install owner must not be changed.
   - Ensure that you use a different database instance from the instance used by the production repository and that you provide the correct connection information when you install.

     For example, under Oracle the `tnsnames.ora` file on the host where the repository copy resides must point to the Oracle instance used by the copy, not the instance used by the production repository.
   - Ensure that the repository copy projects to a connection broker different from the connection broker used by the production repository.
   - Copy all the files from the `$DOCUMENTUM/dba/secure` directory in the source machine to the `$DOCUMENTUM/dba/secure` directory of the target machine.
   - Copy all the files from the `$DOCUMENTUM/data` directory in the source machine to the `$DOCUMENTUM/data` directory of the target machine.
   - Copy the `$DOCUMENTUM/dba/config/<repoName>/dbpasswd.txt` file to the `$DOUCMENTUM/dba/config/<repoName>` directory of the target machine.
   - Copy the `*.cnt` files from the original host to the repository copy host for Federation and replication jobs to work.
3. Apply to the repository copy any patches you applied to the production repository.
4. Connect to the database instance serving the production repository.
5. Use the database vendor's tools to export all objects owned by the repository owner and export the schema for the tables comprising the repository.

   Contact the database vendor for any technical support you would need to use the database tools.
6. On the production repository host's file system, create a backup of the $DOCUMENTUM/data/*repository_name* directory. This is the directory containing the repository's content files.
7. Stop the repository copy.

8. Connect as the database system administrator to the database instance that is serving the repository copy. For example, on Oracle, connect as the System account.
9. Destroy the existing tablespaces or database by using the `dm_DeleteTableSpace.sql` script in $DOCUMENTUM/dba/config/*repository_name*/.

   The scripts are database-specific. Run the script using the tools provided by the database vendor.
10. Delete the physical database file from the file system.

    The name and location of the physical file are in the `dm_CreateTableSpace.sql` script.
11. Create new tablespaces or databases for the repository copy by using the `dm_CreateTableSpace.sql` script in $DOCUMENTUM/dba/config/*repository_name*.

    The scripts are database-specific. Run the script by using the tools provided by the database vendor.
12. Import the database export taken from the production repository into the newly created tablespaces or database.
13. Verify that the database tables have the correct value for the test system host name by checking the following values:

    - r_host_name and web_server_loc in dm_server_config_s
    - host_name in dm_mount_point_s
    - target_server in dm_job_s
    - projection_targets in dm_server_config_r
    - object_name from dm_sysobject_s where r_object_type ='dm_acs_config'
    - acs_base_url in dm_acs_config_r
14. Connect to the database that is serving the repository copy as the repository owner .
15. If any of the values in step 13 are incorrect, use SQL Server to correct the values.
16. Set the server to rebuild the OpenText Documentum CM views with this SQL Server statement:

    ```
    update dm_type_s set views_valid=0
    ```
17. If you are testing operations that require the content files, copy the content file backup from the production repository to the file system of the repository copy.
18. Navigate to the `DOCUMENTUM/dba/config/<repository_name>` directory and open the `server.ini` file in a text editor.
19. Ensure that the preserve_existing_types key in the SERVER_STARTUP section is set to TRUE:

```
preserve_existing_types=T
```

20. Ensure that the crypto configuration parameters are set in the SERVER_STARTUP section.

    - For the repository created on pre-*7.0* version, add the following settings to the `server.ini` file:

      ```
      #RKM configuration parameters
      crypto_mode = 3DES_RSA2048_SHA3_384
      crypto_keystore = Local
      ```

    - For the repository created in *7.x* or *16.x* versions, the settings present in the `server.ini` file on the source machine must be copied to the `server.ini` file of target machine.

21. Save the `server.ini` file.
22. Start Documentum CM Server for the repository copy.
23. Retrieve all the dm_jms_config objects from the repository copy and verify that the base_uri attribute and projection_targets attribute are set correctly.

    a. Start IDQL and connect to the repository as the installation owner.

    b. Run the following command to get a list of all dm_jms_config objects:

    ```
    select * from dm_jms_config
    ```

    c. Run the following command to change each projection target:

    ```
    update dm_jms_config objects set projection_targets[x]='new_target'
    where r_object_id='object_id'
    ```

    d. Run the following command to change each base URI:

    ```
    update dm_jms_config objects set base_uri[x]='new_base_uri'
    where r_object_id='object_id'
    ```

    e. Restart Documentum CM Server for the changes to take effect.

24. If you are testing the migration of a Web content management repository, modify the user objects to reflect the new authentication domain.

    a. Start IDQL and connect to the repository as the installation owner.

    b. Run the following commands:

    ```
    update dm_user objects
    set user_login_domain ='new_machine_name' where
    user_login_domain ='old_machine_name'
    ```

    c. Disconnect from the repository and exit IDQL.

25. If Documentum CM Server and content files of the copy reside on a drive different from the drive used by the production repository, use IDQL to update the file_system_path attribute of the dm_location and dm_mount_point objects to the new location:

```
update dm_location objects
set file_system_path='newpath' where file_system_path='old path'
```

```
update dm_mount_point objects
set file_system_path='newpath' where file_system_path='old path'
```

26. Deactivate all jobs by changing the is_inactive attribute on all job objects to TRUE.

6.5 Migrating data using SQL Server

When migrating data using SQL Server 2008, you can use SQL Server Management Studio to import data or to export data from a source database table to a destination table.

If you use this mechanism for importing or exporting data, you may find that the identity columns of the destination tables do not contain the same identity values as the source tables. This is a known issue with the SQL Server Import and Export wizard. For more information, refer to the *Microsoft* documentation.

To resolve this issue, follow these steps:

1. In the **Column Mappings** dialog box, select the **Enable identity insert** option.
2. Under **Mappings**, select a source table.
3. Select **Create destination table** and then click **Edit SQL**.
4. In the **Create Table SQL Statement** dialog box, replace the CREATE TABLE SQL statement with a SQL statement that includes an IDENTITY clause as shown in the following example:

```
CREATE TABLE [dbo].[stud](
       [roll] [smallint] IDENTITY(1,1) NOT NULL,
       [name] [nvarchar](50) NULL,
CONSTRAINT [PK_stud] PRIMARY KEY CLUSTERED
(
       [roll] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF,
 ALLOW_ROW_LOCKS = ON, ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]
```

Note: Assuming that dbo is the schema name.

5. Click **OK** and then click **OK**.
6. Proceed with the remaining steps in the SQL Server Import and Export wizard.
7. You may need to update the query optimization statistics and recreate indexes to improve the database performance by using the following SQL statements:

```
Exec sp_MSForEachTable 'Update Statistics? WITH FULLSCAN'
```

```
EXEC sp_MSforeachtable @command1="print '?' DBCC DBREINDEX ('?')"
```

For more information on updating statistics, see *Microsoft* documentation. For more information about recreating indexes, see *Microsoft* documentation.

Note: If you are using Windows Server 2008 R2 and see database performance issues, check the **Power Options** settings in the Control Panel. The default

power plan setting of **Balanced** is not recommended for SQL Server because of performance issues. Instead, set the power plan option to **High performance**. For more information, see *Microsoft* documentation.

6.6 Consolidating repositories

You can perform the consolidation of repositories for the same versions of the Documentum CM Server. Documentum CM Server 16.7 and later versions do not support RSA lockbox. If you are using Documentum CM Server 7.2, 7.3, or 16.4, ensure that AEK is residing in the RSA lockbox.

In addition, ensure that the source and target machines have separate database instances of SQL Server. The consolidation of repositories has been tested for the *Windows* SQL Server only.

To consolidate repositories, you must configure the Documentum CM Server on both the source and target machines. On both the machines, you have to set non-default and unique values for repository name and repository ID. In addition, set different and unique names for the AEK key, other than the default values.

For example, on the source machine, set the path for the `Documentum` folder as `C:/DocumentumSource`, repository name as `repo1`, and repository ID as `12345`.

After the configuration of the Documentum CM Server is complete, perform the following steps to consolidate the repositories on both the machines:

1. To migrate the SQL Server backup to the target machine, take the backup of the SQL Server database from SQL Server Management Studio and copy it to the target machine.
2. Copy the backup database file from the source to the target machine. Navigate to the SQL server management studio application of the target machine. Right click **database-restore database** and select the location from where you have copied the backup file.
3. Create new tablespaces or databases for the repository copy by using the `dm_CreateTableSpace.sql` script in **$DocumentumSource/dba/config/<repository_name>**. The scripts are database-specific. Run the script by using the tools provided by the database vendor.
4. Ensure that you record the following environment variables that are set in the source machine in a `.bat` file on the target machine.
   - ClassPath
   - dfcpath
   - DM_HOME
   - DOCUMENTUM
   - JAVA_HOME
   - path

After you create the .bat file on the target machine, ensure that you update the values of the environment variables as per the folders in the target host.

5. Copy the `Documentum` folder from the source host to the target host.

   For example, copy the `C:\DocumentumSource` folder on the source host to the `C:\DocumentumTarget` folder on the target host.

6. On the target host, change the name of the `docbroker.ini`.

   For example, change the name of `docbroker.ini` to `docbrokermig.ini`.

7. On the target host, change the name of the connection broker in the `dm_documentum_config.txt` file.

   For example, if you want to change the name of the connection broker to `Docbroker_Mig`, make the following change in the `dm_documentum_config.txt` file:

   ```
   [DOCBROKER_DocbrokerMig]
   NAME=DocbrokerMig
   ```

8. In the `dfc.properties` file, make the following changes:

   - Change the port of the connection broker from the default value to `1889`.
   - Change the value of `dfc.data.dir` and `dfc.tokenstorage.dir` to the updated folder paths.
   - Change the host name of the connection broker to the host name of the target machine.

9. In the `server.ini` file, make the following changes:

   - Update the path of the `dbpasswd.txt` file.
   - Change the port of the connection broker from the default value to `1889`.
   - Change the value of the `user_auth_target` variable to the host name of the target machine.
   - Change the value of the `[DOCBROKER_PROJECTION_TARGET]` host variable to the host name of the target.

10. Add the names of the connection broker and the repository in `C:\Windows\System32\drivers\etc\services` along with the modified port and the name of the connection broker.

    For example, if you have set the name of the connection broker as `DocbrokerMig`, then make changes as follows:

    ```
    DocbrokerMig            1889/tcp            #docbroker
    DocbrokerMig_s         1890/tcp            #docbroker for secure connect
    dm_reponame                 49625/tcp
    dm_ reponame _s         49626/tcp         #Documentum Docbase Servicerepo256aes
    ```

11. For all versions from 16.7 to 21.1: Modify the default value of the port from `908X` to any other value so that there is no port conflict. Make this modification in the following files:

- %DOCUMENTUM%\jboss<version>\server\DctmServer_MethodServer\configuration\standalone.xml
- %DOCUMENTUM%\jboss<version>\server\DctmServer_MethodServer\configuration\dctm.properties
- %DOCUMENTUM%\jboss<version>\server\DctmServer_MethodServer\configuration\standalone_xml_history\standalone.boot.xml
- %DOCUMENTUM%\jboss<version>\server\DctmServer_MethodServer\configuration\standalone_xml_history\standalone.initial.xml
- %DOCUMENTUM%\jboss<version>\server\DctmServer_MethodServer\configuration\standalone_xml_history\standalone.last.xml
- %DOCUMENTUM%\jboss<version>\server\DctmServer_MethodServer\deployments\acs\lib\configs.jar\jmx.properties
- %DOCUMENTUM%\jboss<version>\server\startMethodServer.cmd
- %DOCUMENTUM%\jboss<version>\server\stopMethodServer.cmd

12. For all versions from 21.2 and later: Modify the default value of the port from 908X to any other value so that there is no port conflict. Make this modification in the following files:

    - %CATALINA_BASE%\conf\server.xml
    - %DOCUMENTUM%\tomcat\server\DctmServer_MethodServer\configuration\dctm.properties
    - %DM_JMS_HOME%\webapps\ACS\WEB-INF\classes\jmx.properties
    - %DM_JMS_HOME%\bin\startMethodServer.cmd
    - %DM_JMS_HOME%\bin\stopMethodServer.cmd

13. For all versions from 16.7 to 21.1: Update the folder names and paths in the following files:

    - %DOCUMENTUM%\jboss<version>\server\serviceConfig\MethodServer\conf\wrapper.conf
    - %DOCUMENTUM%\jboss<version>\server\DctmServer_MethodServer\deployments\ServerApps.ear\DmMethods.war\WEB-INF\web.xml
    - %DOCUMENTUM%\jboss<version>\server\DctmServer_MethodServer\deployments\acs.ear\lib\configs.jar\dfc.properties
    - %DOCUMENTUM%\jboss<version>\server\DctmServer_MethodServer\deployments\acs.ear\lib\configs.jar\log4j2.properties
    - %DOCUMENTUM%\jboss<version>\server\DctmServer_MethodServer\deployments\XhiveConnector.ear\APP-INF\classes\dfc.properties
    - %DOCUMENTUM%\jboss<version>\server\DctmServer_MethodServer\deployments\XhiveConnector.ear\APP-INF\classes\log4j2.properties

- %DOCUMENTUM%\jboss<version>\server\DctmServer_MethodServer\deployments\ServerApps.ear\APP-INF\classes\dfc.properties
- %DOCUMENTUM%\jboss<version>\server\DctmServer_MethodServer\deployments\ServerApps.ear\APP-INF\classes\log4j2.properties
- %DOCUMENTUM%\jboss<version>\bin\dctmServerStatus.bat

14. For all versions from 21.2 and later: Update the folder names and paths in the following files:
    - %DM_JMS_HOME%\webapps\DmMethods\WEB-INF\web.xml
    - %DM_JMS_HOME%\webapps\ACS\WEB-INF\classes\dfc.properties
    - %DM_JMS_HOME%\webapps\DmMethods\WEB-INF\classes\log4j2.properties
    - %DM_JMS_HOME%\webapps\XMLStoreService\WEB-INF\classes\dfc.properties
    - %DM_JMS_HOME%\webapps\XMLStoreService\WEB-INF\classes\log4j2.properties
    - %DM_JMS_HOME%\bin\dctmServerStatus.bat
15. For all versions from 16.7 to 21.1: Update the folder name, port, and host name in the following files:
    - %DOCUMENTUM%\jboss<version>\server\serviceConfig\MethodServer\conf\DmMethodServer.xml
    - %DOCUMENTUM%\jboss<version>\server\DctmServer_MethodServer\deployments\acs.ear\lib\configs.jar\config\acs.properties
    - %DOCUMENTUM%\jboss<version>\server\DctmServer_MethodServer\deployments\acs.ear\lib\configs.jar\config\acsfull.properties
    - %DOCUMENTUM%\product\7.2\bin\xdb.properties
    - %DOCUMENTUM%\jboss<version>\server\DctmServer_MethodServer\deployments\XMLStoreService.ear\XMLStoreService.war\WEB-INF\classes\xmlstore.properties
    - %DOCUMENTUM%\xhive_storage\XhiveDatabase.bootstrap
    - %DOCUMENTUM%\jboss<version>\server\DctmServer_MethodServer\deployments\XhiveConnector.ear\XhiveConnector.war\WEB-INF\web.xml
16. For all versions from 21.2 and later: Update the folder name, port, and host name in the following files:
    - %DM_JMS_HOME%\webapps\ACS\WEB-INF\classes\config\acs.properties
    - %DM_JMS_HOME%\webapps\ACS\WEB-INF\classes\config\acsfull.properties
    - %DOCUMENTUM%\product\7.2\bin\xdb.properties
    - %DM_JMS_HOME%\webapps\WEB-INF\classes\xmlstore.properties

- `%DOCUMENTUM%\xhive_storage\XhiveDatabase.bootstrap`
- `%DM_JMS_HOME%\webapps\WEB-INF\classes\WEB-INF\web.xml`

17. Update the following values in the database tables in the target host:
    - dm_server_config_s in r_host_name
    - dm_server_config_r in app_server_uri
    - dm_acs_config_r in acs_base_url
    - dm_jms_config_s in base_url
    - dm_user_s in user_os_domain
    - dm_user_s in user_login_domain
    - dm_user_s in user_global_unique_id
    - dm_mount_point_s in host_name
    - dm_job_s in target_server

      Note: Update the value of any job that has old host name, method, or parameters.
    - dm_client_rights_s in host_name
    - dm_client_registration_s in host_name
    - dm_extern_store_r in a_storage_param_value
    - dmr_content_s in set_client
    - dm_sysobject_s in r_lock_machine
    - dm_audittrail_s in host_name
    - dm_sysprocess_config_r in base_uri
    - dm_sysprocess_config_r in projection_targets
    - dm_location_s in file_system_path
    - dm_mount_point_s in file_system_path
    - dmr_content_s in set_file
    - dm_method_s in method_verb
    - dm_audittrail_s in attribute_list
    - dm_audittrail_s in string_2
    - dm_sysobject_s in subject
    - dm_type_s in views_valid
18. To start the connection broker, the repository, and the Java Method Server, perform the following step in the same command prompt where you executed the `.bat` file:

```
start %DM_HOME%\bin\dmdocbroker.exe -init_file %DOCUMENTUM%\dba\Docbroker1.ini -
logfile
%DOCUMENTUM%\dba\log\Docbroker1.Docbroker.log -port 1889
```

```
start %DM_HOME%\bin\documentum.exe -docbase_name <repository_name> -security acl -
init_file
%DOCUMENTUM%\dba\config\<repository_name>\server.ini  -install
_owner Administrator -logfile %DOCUMENTUM%\dba\log\<repository_name>.log
```

19. When using Documentum CM Server 7.2, 7.3, or 16.4, if you have enabled the repository with the lockbox option, then it may not come up after the migration. To facilitate the repository with the lockbox enabled, run the following command:

```
dm_crypto_boot -keyname <AEK_key_name> -lockbox <lockbox_name>.lb -lockboxpassphrase
<lockbox_passphrase> -passphrase <AEK_passphrase>
```

To verify, run the following command:

```
dm_crypto_create -check -keyname <AEK_key_name> -lockbox
<lockbox_name>.lb -lockboxpassphrase <lockbox_passphrase> -passphrase
 <AEK_passphrase>
```

If you have used the custom paraphrase, then run the following command:

```
dm_crypto_boot -passphrase <AEK_passphrase> -all
```

6.7 Migrating data from earlier versions of Documentum CM Server

There are no special requirements or considerations when migrating data from earlier versions of Documentum CM Server to 64-bit Documentum CM Server. Follow the standard procedures for your migration utility.

6.8 Using DQL to migrate content to an XML Store

You can migrate XML files from an existing OpenText Documentum CM file store to an XML Store, between XML Stores, and out of an XML Store using an update DQL query. To migrate, run the DQL Query as follows:

```
UPDATE dm_sysobject OBJECTS set a_storage_type = 'xhive_store_01'
```

where a_storage_type = 'filestore_01' and a_content_type = 'xml'

Note: This procedure migrates only the current version of the object.

6.9 Migrating custom Documentum CM Server methods

After upgrading Documentum CM Server, run the configuration tool to configure the internal Java Method Server service. The configuration tool writes the location of the Java methods to the internal method server. The location of the methods directory is written to the `web.xml` file in the method server deployment directory, for example, `%DM_JMS_HOME%\webapps\WEB-INF\lib`:

```
<init-param>
  <param-name>methodlocation-1</param-name>
  <param-value>C:\Documentum\dba\java_methods</param-value>
</init-param>
```

Your custom Documentum CM Server methods located in `%DOCUMENTUM%\dba\java_methods` (Windows) or `$DOCUMENTUM/dba/java_methods` (Linux) continue to work. If you are migrating to a new Documentum CM Server installation, copy the methods from this directory to the same folder location in the new Documentum CM Server installation.

6.10 Migrating DocApps and BOF2 modules

BOF2 modules and DocApps do not need to be changed when you upgrade Documentum CM Server to OpenText Documentum CM 6.0 or later. If you want to change a DocApp or module on an upgraded OpenText Documentum CM 6.0 or later Documentum CM Server, create a project in Documentum Composer and add your BOF2 modules or DocApp. The *OpenText Documentum Content Management - Composer User Guide (EDCPC250400-UGD)* provides more information about working with modules and Documentum Archive (DAR) files.

Note: It is recommended that you use DARs instead of DocApps whenever possible.

Use the Documentum Composer project migration utility to migrate a DocApp or a DocApp archive to a DAR file: **New** > **Project** > **Documentum Project** > **Documentum Project from Repository DocApp**. Documentum Composer generates a DAR file that can be installed in a new instance of Documentum CM Server or edited in place in an upgraded Documentum CM Server instance. The *OpenText Documentum Content Management - Composer User Guide (EDCPC250400-UGD)* provides more information.

If you want your Foundation Java API 5.3 SP6 clients to use upgraded BOF2 modules, perform the following tasks:

1. Compile them for a Java 1.4.x target <javac target=1.4> to make them compatible with older virtual machines.

2. Compile them against Foundation Java API 5.3 SP6 rather than Foundation Java API 6.0 or later to ensure that they do not accidentally reference new interfaces.

To migrate custom Business Objects in an environment of 5.3 SP6 clients that access Documentum CM Server 6.0 or later, perform the following tasks:

- SBO

  Install your 5.3 SP6 DocApps in the 5.3 SP6 global registry. Do not upgrade this global registry.

- Module or TBO

  Make sure that your code works with Foundation Java API 5.3 SP6. It must compile with JDK 1.4.2 and must not use any classes or methods that are new in Foundation Java API 6.0 or later.

6.11 Postmigration tasks

Complete all migration-related tasks described in this chapter. Review and complete the tasks described in the following chapters, if necessary:

- “Migrating Foundation Java API customizations“ on page 203
- “Migrating Foundation SOAP API customizations“ on page 209
- “Migrating Foundation CMIS API customizations“ on page 217
- Appendix A, Migrating DMCL APIs to Foundation Java API on page 225

After completing the migration of the repository, you need to upgrade the repository and Documentum CM Server to 25.x. For more information, see “Upgrading the Documentum CM Server software” on page 44.

Chapter 7

Migrating Foundation Java API customizations

The Documentum Java-Com Bridge (DJCB) and Primary Interop Assembly (PIA) are deprecated from version 6. This chapter describe how to migrate Foundation Java API customizations to version 6.5 SP2 or later.

7.1 Java class changes

New classes, methods, and class members, as well as changed or deprecated methods and members, are documented in the *OpenText Documentum Content Management - Server System Object Reference Guide (EDCCS250400-ORD)* and Foundation Java API *Javadocs*.

7.2 Configuring Foundation Java API for native IPv4 operations

Since version 6.5, to configure Foundation Java API installed on a dual-stack machine for native IPv4 operation, perform the following tasks:

- Specify a host with an IPv4 address in the `dfc.properties` file as the value of `dfc.docbroker.host`.
- Disable the dual-stack operation for JVM.

  A custom property setting in the JVM determines the communications protocol used by the operating system. By default, this custom property `java.net.preferIPv4Stack` is set to `False` to support dual-stack communications. To configure a host for native IPv4, set this property to `True`.

7.3 Configuring 6.7 clients to work with Documentum CM Server 7.x

If you install the version of 6.7 SP2 for the clients such as TaskSpace to work with a fresh Documentum CM Server 7.x, you must perform the following steps to update the dm_bof_registry user password since Documentum CM Server 7.x uses a different encryption algorithm (FIPS/SHA1) than that used by earlier versions of Documentum CM Server (MD5):

1. Decrypt the dm_bof_registry user password using the decrypt API of the RegistryPasswordUtils class in Foundation Java API 7.x to get the plain text password.
2. Encrypt the plain text password using the encrypt API of the RegistryPasswordUtils class in Foundation Java API 6.7 SP2 on the client.

3. Place the encrypted password in `dfc.properties` on the client.

7.4 Migrating customizations to business objects

Since version 6.0, the Business Object Framework (BOF) provides a framework for your customizations that can be accessed from various client applications and service-based architecture. The following kinds of Foundation Java API customizations should be migrated to Business Objects:

- Core custom action execution logic
- Process automation, for example, creating renditions during checkin, creating workflows after checkin
- Custom data handlers
- Helper methods in utility classes, for example, attaching or detaching a lifecycle, promoting or demoting a document
- Business validation, for example, permitting an export operation

7.4.1 Examples of BOF classes

7.4.1.1 Updating attributes of an object based on its location

Generally, you organize documents in a meaningful folder hierarchy. You can also set one or more attributes on an object based on the location in which it is imported or created. The BOF module contains a TBO that sets the attribute after the operation, based on the parent folder.

7.4.1.2 Attaching a lifecycle during a checkin operation

An SBO can be used to perform an operation after checkin, such as attaching a lifecycle. Other possible operations include promoting a workflow or creating a rendition.

7.5 Migrating DMCL API calls to Foundation Java API calls

Since version 6.0, the C++ DMCL API has been replaced with the Java-based Foundation Java API. These core changes, while significant, are largely transparent to the Foundation Java API user. C++ applications that interact directly with the DMCL continue to work as a copy of DMCL continues to be provided. OpenText Documentum CM 6.0 features are not available through DMCL.

Appendix A, Migrating DMCL APIs to Foundation Java API on page 225 provides a map of DMCL APIs to Foundation Java APIs.

7.6 Search service

The Foundation Java API search service replaces prior mechanisms for building and running queries. You can use the IDfQuery interface, which is not part of the search service, for simple queries.

The search service provides the ability to run searches across multiple OpenText Documentum CM repositories and external repositories as well. The Javadocs for the com.documentum.fc.client.search package describe how to use this capability.

7.7 Full format specifications no longer accepted

Since version 6.0, Foundation Java API methods such as setFile that previously accepted a full format specification no longer do so. Those methods accept only a format name, such as txt or word, for the format argument.

7.8 Character string handling improved

In previous releases, if you attempted to set a character string property with a value that exceeded the defined length of the property, Foundation Java API silently truncated the value to the maximum length of the property, then set the property. For OpenText Documentum CM 6.0, Foundation Java API throws an exception instead of truncating the value and setting the property.

To use the pre-OpenText Documentum CM 6.0 behavior, set the `dfc.compatibility.truncate_long_values` property in the `dfc.properties` file to `T`. This property is false, by default.

7.9 Aspects, a new BOF module type for developers

Since version 6.0 supports aspects, a new framework for extending object behavior and attributes. Aspects are a type of BOF entity that can be dynamically attached to object instances in order to provide fields and methods beyond the standard ones for the object type. The extended behavior can include functionality that applies to types across the object hierarchy. For example, an aspect could label objects as retainable or web-viewable, and this single aspect could be applied to multiple distinct object types.

Aspects can speed development and improve code reuse, because the extended attributes and behavior do not alter the underlying type definitions. You can create aspects and associate them with an individual object or an object type. If you associate them with an object type, the aspect is automatically associated with each new object of the specified object type. Aspects can also have properties defined for them. Properties defined for an aspect appear to users as if they are defined for the object type of the object to which the aspect is attached.

7.10 JMX management of DfPreferences and dfc.properties

In J2EE Foundation Java API-based applications, JMX agent, and Managed Bean (MBean) components manage active settings in DfPreferences and persistent settings in `dfc.properties`. The settings are displayed in Documentum Administrator, which separates active settings (in DfPreferences) from persistent settings (in `dfc.properties`).

7.11 Foundation Java API deployment

Foundation Java API is deployed with each application or product that requires it, using a standard J2EE deployment strategy. In the J2EE deployment process, the `dfc.jar` file and related files are packaged in a product's WAR file so that each Foundation Java API instance can have its own Foundation Java API configuration.

7.12 Configuration for AAC tokens

If you are using AAC tokens configured to be valid only when sent from applications on particular host machines, set the `dfc.machine.id` key in the `dfc.properties` file used by those client applications. Set the key to the machine ID of the host from which the AAC token is sent.

7.13 Setting the maximum number of results per source

Administrators can enhance performance by adjusting the maximum number of results returned per source as the result of a query. The default value is 350. The maximum number of results to retrieve is set in the `dfc.properties` file using the `dfc.search.max_results_per_source` parameter as follows:

```
dfc.search.max_results_per_source=<number_of_results>
```

For example:

```
dfc.search.max_results_per_source=350
```

7.14 Foundation Java API does not support linked store storage areas

Since version 6.5, Foundation Java API does not support linked store storage areas. As a consequence, the following items are deprecated:

- The dm_linkedstore object type, which represents linked store storage areas
- The dmi_linkrecord object type, which records the links between a linked storage area and file stores
- The CLEAN_LINKS administration method, which removes orphaned link records, if needed

7.15 External storage

If you are using an external storage area and the plug-in is configured to execute on the client host, reconfigure the plug-in to execute on the server. In 6.5 and later versions, Foundation Java API does not support executing the plug-in on the client. To configure the plug-in to execute on the server, set the a_exec_mode property of the storage object to F (false). The storage object is one of dm_extern_file, dm_extern_free, or dm_extern_url, depending on the type of external storage you are using.

7.16 Foundation Java API does not support optical storage devices

Foundation Java API does not support optical storage devices with version 6.5.

Chapter 8

Migrating Foundation SOAP API customizations

This chapter covers operations you must perform when migrating Foundation SOAP API customizations to Foundation SOAP API 25.4. It also includes functionality and compatibility changes that you must consider after migrating to Foundation SOAP API 25.4.

8.1 Upgrading the Foundation SOAP API .NET productivity layer

The following table provides you with an overview of the supported upgrade paths and the corresponding configurations needed for the upgrade.

Table 8-1: Foundation SOAP API .NET productivity layer upgrade matrix

Original Version	New Version																								
	6.7 SP2 Pn	7.0 Pn	7.1 Pn	7.2 Pn	7.3 Pn	16.4 Pn	16.7 Pn	16.7.1 Pn	20.2 Pn	20.3 Pn	20.4 Pn	21.1 Pn	21.2 Pn	21.3 Pn	21.4 Pn	21.1 Pn	22.2 Pn	22.4 Pn	23.2 Pn	23.4 Pn	24.2 Pn	24.4 Pn	25.2 Pn	25.4 Pn
6.7 SP2 Pm	B	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D
7.0 Pm		B	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D
7.1 Pm			B	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D
7.2 Pm				B	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D

Original Version	New Version																								
	6.7 SP2 Pn	7.0 Pn	7.1 Pn	7.2 Pn	7.3 Pn	16.4 Pn	16.7 Pn	16.7.1 Pn	20.2 Pn	20.3 Pn	20.4 Pn	21.1 Pn	21.2 Pn	21.3 Pn	21.4 Pn	22.1 Pn	22.2 Pn	22.4 Pn	23.2 Pn	23.4 Pn	24.2 Pn	24.4 Pn	25.2 Pn	25.4 Pn
7.3 Pm					B	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D
16.4 Pm						B	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D
16.7 Pm							B	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D
16.7.1 Pm								B	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D
20.2 Pm									B	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D
20.3 Pm										B	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D
20.4 Pm											B	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D
21.1 Pm												B	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D

Original Version	New Version																							
	6.7 SP2 Pn	7.0 Pn	7.1 Pn	7.2 Pn	7.3 Pn	16.4 Pn	16.7 Pn	16.7.1 Pn	20.2 Pn	20.3 Pn	20.4 Pn	21.1 Pn	21.2 Pn	21.3 Pn	21.4 Pn	22.1 Pm	22.2 Pm	22.4 Pm	23.2 Pm	23.4 Pm	24.2 Pn	24.4 Pn	25.2 Pn	25.4 Pn
21.2 Pm													B	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D
21.3 Pm														B	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D
21.4 Pm															B	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D
22.1 Pm																B	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D
22.2 Pm																	B	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D
22.4 Pm																		B	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D
23.2 Pm																			B	A, C, D	A, C, D	A, C, D	A, C, D	A, C, D
23.4 Pm																				B	A, C, D	A, C, D	A, C, D	A, C, D

Original Version	New Version																						
	6.7 SP2 Pn	7.0 Pn	7.1 Pn	7.2 Pn	7.3 Pn	16.4 Pn	16.7 Pn	16.7.1 Pn	20.2 Pn	20.3 Pn	20.4 Pn	21.1 Pn	21.2 Pn	21.3 Pn	21.4 Pn	22.1 Pn	22.2 Pn	22.4 Pn	23.2 Pn	23.4 Pn	24.2 Pn	24.4 Pn	25.2 Pn	25.4 Pn
24.2 Pm																					B	A, C, D	A, C, D	A, C, D
24.4 Pm																						B	A, C, D	A, C, D
25.2 Pm																							B	A, C, D

SP = Service Pack

P = Patch; Pm, Pn = Patch 1, Patch 2, and so on, (m < n)

Option A: recompile – recompile the Foundation SOAP API-based application.

Option B: xcopy – replace old versions with new ones without recompile.

Option C: publisher policy – install new versions to global assembly cache (GAC) and make both versions coexist.

Option D: application/machine configuration – configure the application configuration file or machine configuration file to redirect assemblies. The *Microsoft* documentation provides more information.

The *Microsoft* documentation provides more information about .NET deployment.

8.1.1 Upgrading from 6.7 SP2

To upgrade from 6.7 SP2, you must install the Foundation SOAP API 25.4 productivity layer assemblies to the GAC.

1. Deploy the new Foundation SOAP API 25.4 productivity layer assemblies in one of the following ways:

   - If a working directory does not exist, then install it to the GAC.

     Note: Administrator privileges are required to perform GAC operations.

   - If a working directory does exist, then use the `xcopy` command to copy it to the working directory.

2. Deploy the publisher policy assemblies as follows:

   a. Choose the publisher policy assembly from the Foundation SOAP API SDK with appropriate version.

      For example, if you are upgrading from 7.0 to 25.4, choose the assembly `Policy.7.0.Emc.Documentum.FS.XXX.DLL` from the SDK in the `<dfs_sdk_folder>\lib\dotnet\PublisherPolicy` directory.

   b. Install the publisher policy assembly to the GAC.

      The *Microsoft* documentation provides more information about installing assemblies to the GAC.

3. Complete the tasks as described in "Licensing OpenText Documentum CM" on page 59.

After you have installed the assemblies to the GAC, they are shared by all of the applications on the machine. If you have multiple Foundation SOAP API-based applications on the same machine and you do not want to upgrade Foundation SOAP API for some of them, you can bypass the publisher policy assemblies in those applications by modifying the application configuration file. The *Microsoft* documentation provides more information about bypassing the publisher policy assemblies.

To uninstall the upgraded assemblies from the GAC, you simply delete the assemblies from the GAC. The *Microsoft* documentation provides information about deleting assemblies from the GAC.

8.1.2 Upgrading from a pre-25.4 patch version

To upgrade, use the `xcopy` command to replace your existing Foundation SOAP API .NET productivity layer assemblies in your Foundation SOAP API application's working directory with the new Foundation SOAP API SDK assemblies.

8.2 Restoring trusted certificates after upgrading UCF

In Foundation SOAP API 25.4, UCF expects that JRE 8.0 update 152 or later is installed on the client. If JRE 8.0 update 152 or later is not found on the client, UCF indicates that you must upgrade to JRE 8.0 update 152 or later. In some SSL environments, the UCF client may have imported some trusted certificates to the UCF JRE's cacerts store before the upgrading. These trusted certificates will be lost during the JRE upgrading. Therefore, you have to import the trusted certificates into the cacerts store of the upgraded JRE. To do this, perform the following steps:

1. Encrypt the trust or keystore password:

   a. Navigate to the following directory:

      `Profile}\Documentum\ucf\${HOSTNAME}\shared\bin\8.x.0000.<minor_version>`

   b. Run the following command in the console:

      ```
      java -cp ".\ucf-client-api.jar;.\ucf-client-impl.jar"
       com.documentum.ucf.common.util.spi.BaseCipher <trust or keystore password>
      ```

      Example output:

      ```
      cipher.name: ${cypher.name} cipher.secret.key:
      ${cipher.secret.key} cipher.secret.key.algorithm:
      ${cipher.secret.key.algorithm} Encrypted password
      (e.g. https.truststore.password): ${https.keystore/truststore.password}
      Password encoding (e.g. https.truststore.password.encoding):
      {https.keystore/truststore.password.encoding}
      ```

2. Configure the UCF client:

   a. Locate and open the following configuration file:

      `${User Profile}\Documentum\ucf\${HOSTNAME}\shared\config\ucf.client.config.xml`

   b. Add following options, and then save the file.

      ```
      <configuration name="com.documentum.ucf">
          ....         <option name="https.keystore.file">
                  <value>${https.truststore.file}</value>
              </option>         <option name="https.keystore.password">
                  <value>{https.keystore/truststore.password}</value>
              </option>         <option name="https.keystore.password.encoding">
                  <value>{https.keystore/truststore.password.encoding}</value>
              </option>         <option name="cipher.name">
                  <value>${cypher.name}</value>
              </option>         <option name="cipher.secret.key">
                  <value>${cipher.secret.key}</value>
              </option>         <option name="cipher.secret.key.algorithm">
                  <value>${cipher.secret.key.algorithm}</value>
      ```

```
        </option>         <option name="https.truststore.file">
            <value>${https.truststore.file}</value>
        </option>         <option name="https.truststore.password">
            <value>{https.keystore/truststore.password}</value>
        </option>         <option name="https.truststore.password.encoding">
            <value>{https.keystore/truststore.password.encoding}</value>
        </option>     </configuration>
</configurations>
```

8.3 Trusted login is disabled by default

Foundation SOAP API 7.x enhances the trusted login mechanism for Foundation SOAP API server so that it is disabled by default. Because of this change, users who do not provide the correct password cannot access Foundation SOAP API services in default settings. Foundation SOAP API server enables trusted login only if you explicitly enable it by setting the `dfc.session.allow_trusted_login` property to `true` in the `dfc.properties` file.

8.4 Cookie consistency check

Previously, the Foundation SOAP API client enforced the check of cookie consistency. In Foundation SOAP API 7.x, the Foundation SOAP API server enforces check of cookie consistency.

8.5 .NET framework update

In previous releases, UCF .NET depends on the availability of .NET Framework 3.5 SP1 on the client machine on which the UCF assembly files are downloaded. Starting from Foundation SOAP API 7.x, the client machine must have .NET Framework 4.0 installed to support the .NET UCF integration.

Chapter 9

Migrating Foundation CMIS API customizations

This chapter covers operations you must perform and some functionality and compatibility changes that you must note after migrating to Foundation CMIS API 7.x.

9.1 getFolderParent returns feed

The return type of the `getFolderParent` method is changed to Feed.

Previously, the `getFolderParent` method returned entries. To unify the returns of `getFolderParent` and `getOjectParents`, the `getFolderParent` method now returns feeds. As a result of this change, you have to modify your code for the applications that use the `getFolderParent` method.

Chapter 10

Migration scenarios

This chapter describes some of the supported scenarios for migrating and upgrading a previous version of Documentum CM Server to 25.4.

Note: Although there can be multiple migration scenarios depending on the operating system/database combination, it is not possible to document all of those scenarios. This chapter only covers some of those scenarios that were tested. However, for a particular operating system/database combination, the migration steps do not vary much across Documentum CM Server versions.

10.1 Migrating Documentum CM Server 6.7 SP2 to 25.4 – Windows/SQL Server

This migration scenario provides the step-by-step instructions for migrating and upgrading the 32-bit Documentum CM Server 6.7 SP2 installed on the Windows 2008 SP2 (32-bit) operating system and using SQL Server 2008 SP1 (32-bit) as the database with SQL Server 2008 SP1 (32-bit) client. The migration process must be done in the following sequence:

1. Install 32-bit Documentum CM Server 6.7 SP2 on a target host running Windows 2008 SP2 (64-bit) operating system.
2. Migrate the repository from the source host to the target host.
3. Upgrade the operating system on the target host to Windows Server 2022 (64-bit).
4. Upgrade the database to SQL Server 2017.
5. Upgrade Documentum CM Server to 25.4.

The following table lists the base and upgraded versions of the Documentum CM Server, operating system, and database that are supported in this migration scenario.

Table 10-1: Base and upgraded OS/DB/Documentum CM Server versions

	Base version	Upgraded version
Operating System	Windows Server 2008 SP2 (32-bit)	Windows Server 2022 (64-bit)
Database	SQL Server 2008 SP1 (32-bit) with 32-bit client libraries	SQL Server 2017
Documentum CM Server	32-bit Documentum CM Server 6.7 SP2	64-bit Documentum CM Server 25.4

10.1.1 Pre-migration tasks

1. Back up the repository. If the repository contains customized repository formats (dm_format objects), back up the customized formats.
2. Clean up the repository.
3. Run the Consistency Checker tool. The syntax is:

```
dmbasic -fconsistency_checker.ebs -eEntry_Point -- <repository_name>
<superuser> <password>
```

4. Fix the inconsistencies reported by the Consistency Checker tool as errors.
5. Back up your cleaned, consistent repository.
6. Ensure that filestore_01 is online using any one of the following methods:
   - Using Documentum Administrator, go to the Storage node and verify that filestore_01 shows as online.
   - Dump the filestore and check the r_status attribute:

```
API>retrieve,c,dm_filestore where name='filestore_01' API>dump,c,l
```

7. Execute the following query from SQL Server Management Studio:

```
GRANT VIEW ANY DEFINITION TO "repository user name"
```

10.1.2 Migration tasks

1. On the target host, install Windows 2008 SP2 (32-bit) operating system and the 32-bit SQL Server 2008 SP1 database client libraries.
2. Install the 32-bit Documentum CM Server 6.7 SP2.
3. Copy `%DOCUMENTUM%\dba\secure\aek.key` and `%DOCUMENTUM%\data` from the production repository host to the same locations on the target host.
4. Create a new connection broker on the target host using the Documentum CM Server configuration program.
   a. From `%DM_HOME%\install`, run `Server_Configuration_Program.exe`.
   b. Type the installation owner password and click **Next**.
   c. Select **Custom configuration** and click **Next**.
   d. When you configure a repository, optionally select the check box to enable database partitioning. By default, database partitioning is disabled.
   e. Select the option to configure both connection broker and repository and click **Next**.
   f. Choose **Create a new connection broker** and click **Next**.
   g. Type a connection broker name (default: Docbroker) and the port number on which the connection broker listens, or accept the defaults. The default port is 1489. If you are using the default port number, ensure that the next

port number (1490) is available for use because the connection broker requires that two ports be reserved.

h. Click **Automatic** to have the connection broker automatically start when the host starts, or click **Manual** for manual startup.

i. Select the mode in which the connection broker connects to the repository and click **Next**.

j. To continue with the server configuration, select **Continue with server configuration** and click **Next**.

k. Select **Create a repository** and click **Next**.

5. Configure the repository.

a. Select **Create a new repository** and click **Next**.

b. Click **Next** to accept the default data directory location or browse for a different location.

c. Click **Next** to accept the default share directory location or type a new location.

d. Click **Next** to accept the default fully qualified domain name.

e. To enable data partitioning, select the check box and click **Next**.

f. When you provide the repository information, ensure that you use the same repository name, repository ID, and repository owner name and password as the production repository.

g. Select the authentication domain.

h. Specify whether Documentum CM Server starts automatically or manually and click **Next**.

i. Select the option to use an existing database user account and storage, and click **Next**. You must you the same database instance used by the production repository.

j. On SQL Server, select an ODBC data source.

k. Type the username for an existing database user, the database user password, the database administrator username and password, and then click **Next**.

l. Choose the correct index tablespace or datafile name and click **Next**.

m. Accept or modify the Documentum CM Server initialization values and click **Next**.

n. Configure the data files or data devices.

o. Select the type of mail server, perform the tasks depending on the mail server you select, and click **Next**. *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains detailed information.

p. Decide whether to designate the current repository as a global registry.

q. Accept or modify the repository configuration scripts and click **Next**.

r. Choose whether to restart Documentum CM Server to enable SSL client connections.

s. Specify the port that the XML Store should use and the directory where the XML Store should be created.

t. Click **Finish**.

6. Copy the `%DOCUMENTUM%\dba\config\<repository_name>\dbpasswd.txt` file from production repository host to the same location on the target host after providing the XML Store details.

7. Ensure that the repository configuration completes successfully.

8. Retrieve all the dm_jms_config objects from the repository copy and verify that the `base_uri` attribute and `projection_targets` attribute are set correctly.

   a. Start IDQL and connect to the repository as the installation owner.

   b. Run the following command to get a list of all dm_jms_config objects:

   ```
   select * from dm_jms_config
   ```

   c. Run the following command to change each projection target:

   ```
   update dm_jms_config objects set projection_targets[x]='new_target'
   where r_object_id='object_id'
   ```

   d. Run the following command to change each base URI:

   ```
   update dm_jms_config objects set base_uri[x]='new_base_uri'
   where r_object_id='object_id'
   ```

9. If you are testing the migration of a Web content management repository, modify the user objects to reflect the new authentication domain.

   a. Start IDQL and connect to the repository as the installation owner.

   b. Run the following commands:

   ```
   update dm_user objects
   ```

   ```
   set user_os_domain =’new_machine_name’ where user_os_domain =’old_machine_name’
   ```

   c. Disconnect from the repository and exit IDQL.

10. If Documentum CM Server and content files of the copy reside on a drive different from the drive used by the production repository, use IDQL to update the `file_system_path` attribute of the `dm_location` and `dm_mount_point` objects to the new location:

    ```
    update dm_location objects
    set file_system_path='newpath' where file_system_path='old path'
    update dm_mount_point objects
    set file_system_path='newpath' where file_system_path='old path'
    ```

11. Review the “Migrating Documentum CM Server“ on page 185 and complete the remaining migration-related tasks.

12. Restart Documentum CM Server.

10.1.3 Pre-upgrade tasks

Follow the steps provided in "Pre-upgrade tasks" on page 76.

10.1.4 Upgrade tasks

1. Upgrade the operating system to Windows Server 2022 (64-bit).
2. Upgrade the database to SQL Server 2017.
3. Follow the steps in "Upgrade tasks" on page 77.

10.1.5 Post-upgrade tasks

Follow the steps provided in "Post-upgrade tasks" on page 81.

Appendix A. Migrating DMCL APIs to Foundation Java API

This appendix provides information that can help you migrate a DMCL-based application to a Foundation Java API application. Refer to the product *Release Notes* for any known limitations or exceptions to the material in this appendix.

A.1 Overview

There are essentially three languages used: Java, DocBasic, and C++.

If you are using Java for your customizations, they continue to work in OpenText Documentum CM 6.5 or later. There have been no changes to the methods or interfaces of existing classes.

In previous releases, DocBasic applications accessed the DMCL via `dmcl40.dll` (on Windows). In OpenText Documentum CM 6.5 or later, DocBasic applications automatically access the new `dmcl.dll`, which passes instructions back and forth to Foundation Java API via an emulator.

C++ accesses DMCL through dynamic links. The applications continue to work, but they are working with, in essence, the 6.0 version of DMCL (with some bug fixes). C ++ applications using the `dmcl40.dll` do not have access to methods or interfaces introduced in version 6.5.

A.2 Methods with no corresponding Foundation Java API method

The following methods are not implemented in Foundation Java API 6.5 and later:

- Listmessage
- Lpq
- Reset
- Unprint

A.3 Methods with corresponding Foundation Java API methods

"DMCL API methods and corresponding Foundation Java API methods" on page 226 lists the DMCL API methods and the corresponding Foundation Java API methods.

The listing is intended to help you migrate a DMCL-based application to Foundation Java API.

It is not intended as a complete listing of all Foundation Java API methods.

Table A-1: DMCL API methods and corresponding Foundation Java API methods

DMCL API method	Foundation Java API correspondence	
	Interface	Method name
Abort, for transactions	IDfSession IDfSessionManager	abortTrans abortTransaction
Abort, for work flow	IDfWorkflow	abort
Acquire	IDfWorkItem	acquire
Addigsignature	IDfSysObject	addDigitalSignature
Addesignature	IDfSysObject	addESignature
Addactivity	IDfProcess	addActivity
Addlink	IDfProcess	addLink
Addnote	IDfSysObject IDfPackage	addNote appendNote
Addpackage	IDfWorkflow IDfWorkitem	addPackage addPackageEx
Addpackageinfo	IDfActivity	addPackageInfo, addPackageInfoEx
Addport	IDfActivity	addPort
Addrendition	IDfSysObject	addRendition, addRenditionEx, addRenditionEx2, addRenditionEx3,
Addroutecase	IDfActivity	addRouteCase, addConditionRouteCase
Anyevents	IDfSession	hasEvents

DMCL API method	Foundation Java API correspondence	
	Interface	Method name
Append	IDfTypedObject	appendBoolean, appendInt, appendDouble, appendId, appendString, appendTime, appendValue
Appendcontent	IDfSysObject	appendContent, appendContentEx
Appendfile	IDfSysObject	appendFile
Appendpart	IDfSysObject	appendPart
Appendstate	IDfPolicy	appendState
Apply	IDfSession, IDfQuery	apply, in IDfSession execute, in IDfQuery
Archive	IDfSession	archive
Assemble	IDfSysObject	assemble
Assume	IDfSession	assume
Attach	IDfSysObject	attachPolicy, detachPolicy
Audit	IDfAuditTrailManager	registerEventForType, registerEventForObject, registerEvents, register EventsFromQuery, registerEventsInFolder
Authenticate	IDfClient IDfSession IDfSessionManager	authenticate
Begintran	IDfSession IDfSessionManager	beginTrans beginTransaction
Bindfile	IDfSysObject	bindFile
Branch	IDfSysObject	branch
Cachequery	IDfQuery	execute
Changepassword	IDfSession	changePassword
Checkin	IDfSysObject	checkin
Checkinapp	IDfSysObject	checkinEx
Checkout	IDfSysObject	checkout, checkoutEx
Close	IDfCollection	close

DMCL API method	Foundation Java API correspondence	
	Interface	Method name
Commit	IDfSession IDfSessionManager	commitTrans commitTransaction
Complete	IDfWorkitem	complete, completeEx, completeEx2
Connect	IDfSessionManager IDfClient	newSession
Count	IDfTypedObject	getAttrCount
Create	IDfSession	newObject, newObjectWithType
Createaudit	IDfAuditTrailManager	createAudit
Datatype	IDfTypedObject	getAttrDataType
Delegate	IDfWorkitem	delegateTask
Demote	IDfSysObject	demote, scheduleDemote, cancelScheduleDemote
Dequeue	IDfSession	dequeue
Dereference	IDfReplica IDfMirror	dereferenceReplica dereferenceMirror
Describe	IDfSession	describe
Destroy	IDfPersistentObject	destroy
Disassemble	IDfSysObject	disassemble
Disconnect	IDfSession IDfSessionManager	disconnect (in IDfSession) release (in IDfSessionManager)
Dump	IDfTypedObject	dump
Dumpconnection	IDfSessionManager	Use getStatistics method in IDfSessionManager to return an IDfStatisticsManger object, which has the getDocbases and getSessions methods, which return information equivalent to that returned by Dumpconnection
Dumploginticket		
Encryptpass	IDfClient	encryptPassword
Execquery	IDfQuery	execute

DMCL API method	Foundation Java API correspondence	
	Interface	Method name
Execsql		
Execute	IDfWorkflow	execute
Fetch	IDfSession	getObject, getObjectWithCaching
Flush	IDfSession	flush
Flushcache	IDfSession	flushCache
Flushconnectpool	IDfSessionManager	clearIdentities
Freeze	IDfSysObject	freeze
Get	IDfTypedObject	getBoolean, getInt, getDouble, getId, getString, getTime, getValue getRepeatingBoolean, getRepeatingInt, getRepeatingDouble, getRepeatingId, getRepeatingString, getRepeatingTime, getRepeatingValue
Getconnection	IDfSessionManager	newSession
Getcontent	IDfSysObject	getContent
Getdocbasemap	IDfDocbrokerClient	getDocbaseMap getDocbaseMapFromSpecificDocbroker
Getdocbrokermap	IDfDocbrokerClient	getDocbrokerMap
Getevents	IDfSession	getEvents
Getfile	IDfSysObject	getFile, getFileEx, getFileEx2
Getlastcoll	IDfSession	getLastCollection
Getlogin	IDfSession	GetLoginTicket, getLoginTicketEx, getLoginTicketForUser
Getmessage	IDfSession	getMessage
Getpath	IDfSysObject	getPath, getPathEx, getPathEx2
Getservermap	IDfDocbrokerClient	getServerMap getServerMapFromSpecificDocbroker

DMCL API method	Foundation Java API correspondence	
	Interface	Method name
Grant	IDfSysObject	grant, see also grantPermit
Halt	IDfWorkflow	halt, haltEx, haltAll
Id	IDfSession IDfTypedObject	getIdByQualification (in IDfSession) getObjectId (in IDfTypedObject)
Initcrypto	IDfClient	initCrypto
Insert	IDfTypedObject	insertBoolean, insertInt, insertDouble, insertId, insertString, insertTime, insertValue
Insertcontent	IDfSysObject	insertContent, insertContentEx
Insertfile	IDfSysObject	insertFile, insertFileEx
Insertpart	IDfSysObject	insertPart
Insertstate	IDfPolicy	insertState
Install	IDfActivity, IDfPolicy, IDfProcess	install
Invalidate	IDfActivity, IDfPolicy, IDfProcess	invalidate
Iscached		
Kill	IDfSession	killSession (for sessions) flushObject (for SysObjects)
Link	IDfSysObject	link
Listconnection	IDfSessionManager	Use getStatistics method in IDfSessionManager to return an IDfStatisticsManager object, which has the getDocbases and getSessions methods, which return information equivalent to that returned by Listconnection
Locate	IDfTypedObject	findBoolean, findInt, findDouble, findId, findString, findTime, findValue

DMCL API method	Foundation Java API correspondence	
	Interface	Method name
Lock	IDfPersistentObject	lock
Mark	IDfSysObject	mark
Mount	IDfSysObject	mount
Movestate	IDfPolicy	moveState
Next	IDfCollection	next
Offset	IDfTypedObject	findAttrIndex
Pause	IDfWorkitem	pause
Print	IDfSysObject	print
Promote	IDfSysObject	promote, schedulePromote, cancelSchedulePromote
Prune	IDfSysObject	prune
Publish_dd	IDfSession	publishDataDictionary
Purgelocal	IDfSession	purgeLocalFiles
Query_cmd	IDfQuery	execute
Query	IDfQuery	execute
Queue	IDfSysObject IDfWorkflow IDfWorkitem	queue
Readquery	IDfQuery	execute
Refresh	IDfReplica IDfMirror	refreshReplica refreshMirror
Register	IDfSysObject	registerEvent
Reinit	IDfSession	reinit
Remove	IDfTypedObject	remove
Removeactivity	IDfProcess	removeActivity
Removecontent	IDfSysObject	removeContent
Removelink	IDfProcess	removeLink
Removenote	IDfSysObject	removeNote
Removepackage	IDfWorkitem	removePackage
Removepackageinfo	IDfActivity	removePackageInfo
Removepart	IDfSysObject	removePart
Removeport	IDfActivity	removePort

DMCL API method	Foundation Java API correspondence	
	Interface	Method name
Removerendition	IDfSysObject	removeRendition, removeRenditionEx, removeRenditionEx2
Removeroutecase	IDfActivity	removeRouteCase
Removestate	IDfActivity	removeState
Repeat	IDfWorkitem	repeat
Repeating	IDfTypedObject	isAttrRepeating
Resolvealias	IDfSysObject IDfSession	resolveAlias
Restart	IDfSession IDfWorkflow	restart restartAll (for work flow)
Restore	IDfSession	restore
Resume	for lifecycles: IDfSysObject IDfworkflow IDfWorkitem	resume, scheduleResume, cancelScheduleResume (IDfSysObject) resume, resumeAll (IDfWorkflow) resume (IDfWorkitem)
Retrieve	IDfSession IDfTypedObject	getIdByQualification (in IDfSession) getObjectId (in IDfTypedObject)
Revert	IDfPersistentObject	revert
Revoke	IDfSysObject	revoke see also revokePermit
Save	IDfPersistentObject	save
Saveasnew	IDfSysObject	saveAsNew
Seek	IDfContentCollection	seek, seekEx

DMCL API method	Foundation Java API correspondence	
	Interface	Method name
Set	IDfTypedObject	setBoolean, setInt, setDouble, setId, setString, setTime, setValue setRepeatingBoolean, setRepeatingInt, setRepeatingDouble, setRepeatingId, setRepeatingString, setRepeatingTime, setRepeatingValue
Setbatchhint	IDfSession	setBatchHint
Setcontent	IDfSysObject	setContent, setContentEx, setContentEx2
Setcontentattrs		setContentAttrs
Setdoc	IDfSysObject	setIsVirtualDocument
Setfile	IDfSysObject	setFile, setFileEx
Setoutput	IDfWorkitem	setOutput, setOutputByActivities
Setpath	IDfSysObject	setPath
Setperformers	IDfWorkflow	setPerformers
Setpriority	IDfWorkitem	setPriority
Setsupervisor	IDfWorkflow	updateSupervisorName
Shutdown	IDfSession	shutdown
Signoff	IDfPersistentObject	signoff
Suspend	IDfSysObject	suspend, scheduleSuspend, cancelScheduleSuspend
Trace	IDfSession	TraceDMCL
Truncate	IDfTypedObject	removeAll, truncate
Type	IDfSession	getTypeDescription
Unaudit	IDfAuditTrailManager	unRegisterEvent, unRegisterEventForType, unregisterEvents, unRegisterEventsFromQuery, unRegisterEventsInFolder, unRegisterAllEvents
Unfreeze	IDfSysObject	unfreeze
Uninstall	IDfActivity, IDfPolicy, IDfProcess	uninstall

DMCL API method	Foundation Java API correspondence	
	Interface	Method name
Unlink	IDfSysObject	unLink
Unlock	IDfSysObject	cancelCheckOut
Unmark	IDfSysObject	unMark
Unregister	IDfSysObject	unRegisterEvent
Updatepart	IDfSysObject	updatePart, updatePartEx
Useacl	IDfSysObject	useACL
Validate	IDfActivity, IDfPolicy, IDfProcess	validate, validateProcessAndActivities
Values	IDfTypedObject	getValueCount
Vdmpath	IDfObjectPath	getAccessPath, getAccessibleFolderIds
Vdmpathdql	IDfObjectPath	getAccessPath, getAccessibleFolderIds
Verifyaudit	IDfPersistentObject	verifyAudit
Verifyesignature	IDfSysObject	verifySignature

Appendix B. Object type and property changes

These tables describe types and properties that are new, changed, deprecated, or obsolete since OpenText Documentum CM 6.7 SP1.

B.1 New object types

"New object types" on page 235 lists the new object types in OpenText Documentum CM 7.x.

Table B-1: New object types

Type name	Description	Properties
dmc_bpm_lsm	Models a synchronizing split-join block (LSM) within a workflow template.	• join_act • process_id • start_act • step_act
dmc_mq_config	Defines the configuration object of a message queue. An instance of dmc_mq_config is created when a message queue is created.	• queue_name • max_redeliveries • retain_dead_message • retain_period • expiration_interval • default_priority • delivery_timeout • queue_users • permissions

B.2 Changed object types

"Changed object types" on page 235 lists the properties that have their lengths extended in OpenText Documentum CM 7.x.

Table B-2: Changed object types

Type Name	Properties	Data type	Description
dm_user	user_name	char(255)	Length of the property has been extended from 32 to 255.
	user_group_name	char(255)	Length of the property has been extended from 32 to 255.

Type Name	Properties	Data type	Description
	user_login_name	char(255)	Length of the property has been extended from 80 to 255.
	acl_domain	char(255)	Length of the property has been extended from 32 to 255.
	user_admin	char(255)	Length of the property has been extended from 32 to 255.
	user_delegation	char(255)	Length of the property has been extended from 32 to 255.
	default_folder	char(450) for SQL Server, char(740) for Oracle	Length of the property has been extended.
	user_ldap_dn	char(512)	Length of the property has been extended from 256 to 512. This property is deprecated.
dm_group	group_name	char(255)	Length of the property has been extended from 32 to 255.
	owner_name	char(255)	Length of the property has been extended from 32 to 255.
	group_admin	char(255)	Length of the property has been extended from 32 to 255.
	group_global_unique_id	char(400)	Length of the property has been extended from 255 to 400.

Type Name	Properties	Data type	Description
	users_names	char(255)	Length of the property has been extended from 32 to 255. Forms a composite index with r_object_id.
	groups_names	char(255)	Length of the property has been extended from 32 to 255. Forms a composite index with r_object_id.
	i_supergroups_names	char(255)	Length of the property has been extended from 32 to 255. Used in an index by itself.
	i_nondyn_supergroups_names	char(255)	Length of the property has been extended from 32 to 255. Forms a composite index with r_object_id.
dm_sysobject	r_modifier	char(255)	Length of the property has been extended from 32 to 255. Used in an index by itself.
	owner_name	char(255)	Length of the property has been extended from 32 to 255. Used in an index by itself.
	group_name	char(255)	Length of the property has been extended from 32 to 255.
	r_lock_owner	char(255)	Length of the property has been extended from 32 to 255.
	acl_domain	char(255)	Length of the property has been extended from 32 to 255. Forms a composite index with acl_name.

Type Name	Properties	Data type	Description
	r_creator_name	char(255)	Length of the property has been extended from 32 to 255.
dm_acl	owner_name	char(255)	Length of the property has been extended from 32 to 255. Forms two composite indexes: one with (i_partition, object_name) and another with (object_name, r_object_id, i_partition).
	r_accessor_name	char(255)	Length of the property has been extended from 32 to 255.
dmi_package	r_note_writer	char(255)	Length of the property has been extended from 32 to 255.
dmi_queue_item	supervisor_name	char(255)	Length of the property has been extended from 32 to 255.
	sent_by	char(255)	Length of the property has been extended from 32 to 255.
	dequeued_by	char(255)	Length of the property has been extended from 32 to 255. Forms one composite index with (name, sign_off_user, task_state, priority, date_sent).

Type Name	Properties	Data type	Description
	sign_off_user	char(255)	Length of the property has been extended from 32 to 255. Form two composite indexes: one with (name, dequeued_by, task_state, priority, date_sent) and another with (item_id, task_state, name, priority, date_sent, r_object_id).
	name	char(255)	Length of the property has been extended from 32 to 255.
dmi_registry	user_name	char(255)	Length of the property has been extended from 32 to 255.
dmi_wf_attachment	r_creator_name	char(255)	Length of the property has been extended from 32 to 255.
dm_alias_set	owner_name	char(255)	Length of the property has been extended from 32 to 255.
dm_audit_policy	accessor_name	char(255)	Length of the property has been extended from 32 to 255.
dm_type	group_name	char(255)	Length of the property has been extended from 32 to 255.
	owner	char(255)	Length of the property has been extended from 32 to 255.
	group_global_unique_id	char(400)	Length of the property has been extended from 255 to 400.

Type Name	Properties	Data type	Description
dmi_type_info	default_group	char(255)	Length of the property has been extended from 27 to 255.
	acl_domain	char(255)	Length of the property has been extended from 32 to 255.
dm_ftindex_agent_config	queue_user	char(255)	Length of the property has been extended from 64 to 255.
dm_registered	table_owner	char(255)	Length of the property has been extended from 64 to 255.
dm_activity	performer_name	char(255)	Length of the property has been extended from 66 to 255.
dm_workitem	r_performer_name	char(255)	Length of the property has been extended from 32 to 255.
	r_ext_performer	char(255)	Length of the property has been extended from 32 to 255.
dm_audittrail	user_name	char(255)	Length of the property has been extended from 32 to 255.
	owner_name	char(255)	Length of the property has been extended from 32 to 255.
	acl_domain	char(255)	Length of the property has been extended from 32 to 255.
dm_audittrail_acl	accessor_name	char(255)	Length of the property has been extended from 32 to 255.

Type Name	Properties	Data type	Description
dm_audittrail_group	group_admin	char(255)	Length of the property has been extended from 32 to 255.
	users_names	char(255)	Length of the property has been extended from 32 to 255.
	groups_names	char(255)	Length of the property has been extended from 32 to 255.
dm_category	category_owner	char(255)	Length of the property has been extended from 32 to 255.
dm_category_assign	modifier	char(255)	Length of the property has been extended from 32 to 255.
	pre_modifier	char(255)	Length of the property has been extended from 32 to 255.
dm_ci_config	auto_user	char(255)	Length of the property has been extended from 32 to 255.
	manual_user	char(255)	Length of the property has been extended from 32 to 255.
dm_client_rights	allowed_roles	char(255)	Length of the property has been extended from 32 to 255.
dm_docbase_config	a_bpaction_run_as	char(255)	Length of the property has been extended from 32 to 255.
dm_docset_run	run_owner	char(255)	Length of the property has been extended from 32 to 255.

Type Name	Properties	Data type	Description
dm_message_address	user_name	char(255)	Length of the property has been extended from 32 to 255. This type has been changed to registered table.
dm_partition_scheme	owner_name	char(255)	Length of the property has been extended from 32 to 255.
dm_qual_comp	valid_groups	char(255)	Length of the property has been extended from 32 to 255.
dm_reference	r_ref_creator	char(255)	Length of the property has been extended from 32 to 255.
	i_ref_acl_domain	char(255)	Length of the property has been extended from 32 to 255.
dm_router	supervisor_name	char(255)	Length of the property has been extended from 32 to 255.
	task_owner	char(255)	Length of the property has been extended from 32 to 255.
	r_task_user	char(255)	Length of the property has been extended from 32 to 255.
	r_sign_off_user	char(255)	Length of the property has been extended from 32 to 255.
dm_server_config	operator_name	char(255)	Length of the property has been extended from 32 to 255.
	r_install_owner	char(255)	Length of the property has been extended from 32 to 255.

Type Name	Properties	Data type	Description
dm_webc_config	notification_user	char(255)	Length of the property has been extended from 32 to 255.
dm_webc_target	transfer_user	char(255)	Length of the property has been extended from 32 to 255.
dm_workflow	r_creator_name	char(255)	Length of the property has been extended from 32 to 255.
	supervisor_name	char(255)	Length of the property has been extended from 32 to 255.
	r_last_performer	char(255)	Length of the property has been extended from 32 to 255.
	r_performers	char(255)	Length of the property has been extended from 32 to 255.
dmc_completed_workflow	creator_name	char(255)	Length of the property has been extended from 32 to 255.
	supervisor_name	char(255)	Length of the property has been extended from 32 to 255.
dmc_completed_workitem	performer_name	char(255)	Length of the property has been extended from 32 to 255.
dmc_module	a_privilege_roles	char(255)	Length of the property has been extended from 32 to 255.
dmc_wfsdrp_parent	performer_name	char(255)	Length of the property has been extended from 32 to 255.

Type Name	Properties	Data type	Description
dmc_workqueue_policy	owner_name	char(255)	Length of the property has been extended from 32 to 255.
dmc_workqueue_doc_profile	owner_name	char(255)	Length of the property has been extended from 32 to 255.
dmc_workqueue_user_profile	user_name	char(255)	Length of the property has been extended from 32 to 255.
	owner_name	char(255)	Length of the property has been extended from 32 to 255.
dmc_wq_user_skill	user_name	char(255)	Length of the property has been extended from 32 to 255.

B.3 Changed object types with new properties

"New object properties" on page 244 lists the new properties added to existing object types in OpenText Documentum CM 7.x.

Table B-3: New object properties

Type Name	Properties	Data type
dm_ftquery_subscription	zone_value	integer
dm_user	root_log_dir	char(255)
dm_type	r_creation_date	time
	r_modified_date	time
Dm_acs_config	dormancy_status	string(32)
Dm_activity	activity_urn	string(512)
	lsm_id	ID
Dm_docbase_config	dormancy_status	string(32)
	i_crypto_keys_expiry_date	time
	i_expired_crypto_keys	string(255)
	r_crypto_keystore	string(32)

Type Name	Properties	Data type
	r_crypto_mode	string(64)
Dm_ldap_config (this property is deprecated)	group_tree_sync	Boolean
Dm_process	system_name	string(512)
Dmr_content	content_state	integer
Dmi_wf_timer	r_is_initialized	integer
Dmi_change_record	dormancy_change_count	integer
Dmi_workitem	a_control_instruction	string(32)

The *OpenText Documentum Content Management - Server System Object Reference Guide (EDCCS250400-ORD)* provides additional information about the new, changed, deprecated, and obsolete object types and properties.

Appendix C. dfc.properties

C.1 Overview

In version 6.0, Foundation Java API replaced the Server API as the API for Documentum CM Server. As part of this change, the `dmcl.ini` file became obsolete and its relevant entries were migrated to the `dfc.properties` file. In addition, the naming conventions for entries in the `dfc.properties` file were standardized. This appendix describes the changes to the `dfc.properties` file.

C.2 Changes to existing key names

"Name changes for existing dfc.properties since version 6.5 and dfc.new properties" on page 247, describes the changes to existing key names. Both new and old names are listed. For backward compatibility, both new and old names continue to work in OpenText Documentum CM 7.x. Invalid entries do not generate an error, but have no effect on functionality.

Table C-1: Name changes for existing dfc.properties since version 6.5 and dfc.new properties

Old name	New name
dfc.acs.avail.refresh.frequency	dfc.acs.avail.refresh_interval
dfc.acs.config.refresh.frequency	dfc.acs.config.refresh_interval
dfc.admin.ldif.file.charset	dfc.admin.ldif_file_charset
dfc.cacs.check.http.method	dfc.bocs.check.http_method
dfc.cacs.check.keep.number	dfc.bocs.check.keep_number
dfc.cache.append.name	dfc.bof.cache.append_name
dfc.bof.cacheconsistency.interval	dfc.bof.cache.currency_check_interval
dfc.bof.registry.connect.attempt.interval	dfc.globalregistry.connect_attempt_interval
dfc.bof.registry.preload.enabled	dfc.bof.cache.enable_preload
dfc.bof.registry.password	dfc.globalregistry.password
dfc.bof.registry.repository	dfc.globalregistry.repository
dfc.bof.registry.username	dfc.globalregistry.username
dfc.cache.ddinfo.globalCacheSize	dfc.cache.ddinfo.size
dfc.cache.dir	dfc.cache_dir
client_cache_size	dfc.cache.object.size
dfc.cache.query.globalCacheSize	dfc.cache.query.size
dfc.core.truncate_long_values	dfc.compatibility.truncate_long_values

Old name	New name
dfc.config.timeout	dfc.config.check_interval
dfc.checkout.dir	dfc.data.checkout_dir
dfc.data.dir	dfc.data.dir
dfc.docbase.max_deadlock_retries	dfc.session.max_deadlock_retries
dfc.docbase.max_error_retries	dfc.session.max_error_retries
dfc.exception.include_decoration	No change
dfc.exception.include_id	No change
dfc.export.dir	dfc.data.export_dir
dfc.housekeeping.cleanup.interval, dfc.resources.cleanup_interval	dfc.bof.cache.cleanup_interval
dfc.max.vdm.children.flush.count	dfc.vdm.max_child_flush_count
dfc.recordInlineDescendants	dfc.xml.record_inline_descendants
dfc.registry.file	No change
dfc.registry.mode	No change
dfc.resources.diagnostics.enabled	dfc.diagnostics.resources.enable
dfc.search.docbase.brokers	dfc.search.docbase.broker_count
dfc.search.ecis.adapter.domain	dfc.search.external_sources.adapter.domain
dfc.search.ecis.broker_count, dfc.search.ecis.brokers	dfc.search.external_sources.broker_count
dfc.search.ecis.enable	dfc.search.external_sources.enable
dfc.search.ecis.host	dfc.search.external_sources.host
dfc.search.ecis.password	dfc.search.external_sources.password
dfc.search.ecis.port	dfc.search.external_sources.port
dfc.search.ecis.request_timeout, dfc.search.ecis.access.timeout	dfc.search.external_sources.request_timeout
dfc.search.ecis.rmi_name, dfc.search.ecis.name	dfc.search.external_sources.rmi_name
dfc.search.ecis.username, dfc.search.ecis.login	dfc.search.external_sources.username
dfc.search.formatcache.timeout	dfc.search.formatcache.refresh_interval
dfc.search.fulltext.enabled	dfc.search.fulltext.enable
dfc.search.sourcecache.timeout	dfc.search.sourcecache.refresh_interval
dfc.search.typecache.timeout	dfc.search.typecache.refresh_interval
None	dfc.search.matching_terms_computing.enable

Old name	New name
dfc.session.dynamic_delay	No change
dfc.session.pool.enabled, connect_pooling_enabled	dfc.session.pool.enable
dfc.session.pool.timeout	dfc.session.pool.expiration_interval
dfc.session.surrogate.check.interval	dfc.session.surrogate.check_interval
dfc.session.surrogate.mode	No change
dfc.storagepolicy.diagnostics.enabled	dfc.storagepolicy.enable
dfc.storagepolicy.ignore.rule.errors	dfc.storagepolicy.ignore_rule_errors
dfc.storagepolicy.validation.interval	dfc.storagepolicy.validation_interval
dfc.strictURI	dfc.xml.use_strict_uri
dfc.tracing.baseTraceFileName	dfc.tracing.file_prefix
dfc.tracing.enabled, r_trace_level	dfc.tracing.enable
dfc.tracing.entrancePointExprs	dfc.tracing.method_name_filter
dfc.tracing.loggingMode	dfc.tracing.file_creation_mode
dfc.tracing.maxFileSize	dfc.tracing.max_file_size
dfc.tracing.mode	No change
dfc.tracing.stackDepth	dfc.tracing.max_stack_depth
dfc.tracing.threadNameExprs	dfc.tracing.thread_name_filter
dfc.tracing.timestampDateFormat	dfc.tracing.date_format
dfc.tracing.traceFileDirectory	dfc.tracing.dir
dfc.tracing.userNameExprs	dfc.tracing.user_name_filter
dfc.user.dir	dfc.data.user_dir
dfc.validation.expr.currency.check	dfc.validation.expr.currency_check_interval
dfc.validation.expr.debug.all	No change
dfc.validation.expr.debug.code	No change
dfc.validation.expr.debug.eval	No change
dfc.validation.expr.debug.tree	No change
dfc.validation.expr.disable_java	No change
dfc.validation.overrides.currency.check	dfc.validation.overrides.currency_check_interval
dfc.session.recycle_interval, connect_recycle_interval	dfc.session.reuse_limit
None	dfc.validation.allow.empty_string.list_complete

Old name	New name
None	dfc.search.xquery.option.parallel_execution.enable
None	dfc.session.load_balance_strategy
None	dfc.session.max_server_choice_age
None	dfc.session.keepalive.enable
None	dfc.connection.unused_connection_timeout
None	dfc.xml.suppress_default_namespace_decl
None	dfc.internal.purge_far_connections
Note: Compatibility is ensured with previous properties that refer to `ecis`.	

C.3 dmcl.ini key migration to dfc.properties

"dfc.properties keys migrated from dmcl.ini file" on page 250 describes the `dmcl.ini` keys that migrated to the `dfc.properties` file since OpenText Documentum CM 6.5.

Table C-2: dfc.properties keys migrated from dmcl.ini file

dmcl.ini key	Corresponding new dfc.properties key
application_code	dfc.application_code
batch_hint_size	dfc.batch_hint_size
backup_host	dfc.docbroker.host
backup_port	dfc.docbroker.port
backup_protocol	dfc.docbroker.protocol
backup_service	dfc.docbroker.service
backup_timeout	dfc.docbroker.timeout
castore_write_max_attempts	dfc.content.castore.max_write_attempts
castore_write_sleep_interval	dfc.content.castore.write_sleep_interval
client_date_format	dfc.date_format
client_locale	dfc.locale
connect_pooling_enabled	dfc.session.pool.enable
connect_retry_limit	dfc.session.max_connect_retries
ini_file_path	dfc.config.file
local_clean_on_init	dfc.data.local_clean_on_init
local_diskfull_limit	dfc.data.local_diskfull_limit

dmcl.ini key	Corresponding new dfc.properties key
local_path	dfc.data.local_dir
local_purge_on_diskfull	dfc.data.local_purge_on_diskfull
max_session_count	dfc.session.max_count*
primary_host	dfc.docbroker.host
primary_port	dfc.docbroker.port
primary_protocol	dfc.docbroker.protocol
primary_service	dfc.docbroker.service
primary_timeout	dfc.docbroker.timeout
ref_binding_label	dfc.reference.binding_label
secure_connect_default	dfc.session.secure_connect_default
token_storage_path	dfc.tokenstorage.dir
token_storage_enabled	dfc.tokenstorage.enable
umask	dfc.data.umask
use_compression	dfc.content.use_compression
use_content_server	dfc.content.use_content_server

*The settings from `dmcl.ini` from your current configuration are transferred after an upgrade. This might cause an issue if the `dmcl.ini` property `dfc.max_session_count` is set to a low session count. It is recommended that you remove this property setting from the `dmcl.ini` file before performing an upgrade.

C.4 Obsolete dmcl.ini and session configuration options

"Obsolete session configuration options" on page 251 lists the `dmcl.ini` keys that are obsolete since OpenText Documentum CM 6.5 and have no equivalent to set in `dfc.properties`. It also lists properties formerly present in the session configuration objects that are obsolete in OpenText Documentum CM 6.5 and later versions.

Table C-3: Obsolete session configuration options

Entry	Source	Comments
block_during_rpc	dmcl.ini	Is specific to native code DMCL.
client_codepage	dmcl.ini	none
client_os_codepage	dmcl.ini	none
connect_callback_enabled	api config and session config objects	none

Entry	Source	Comments
connect_failure_callback	api config and session config objects	none
connect_failure_data	api config and session config objects	none
connect_success_callback	api config and session config objects	none
connect_success_data	api config and session config objects	none
content_callback_data	api config and session config objects	none
content_callback_function	api config and session config objects	none
local_diskfull_warn	dmcl.ini	none
network_callback_data	api config and session config objects	none
network_callback_function	api config and session config objects	none
new_connection_callback		none
new_connection_data		none
nfs_enabled	dmcl.ini	
r_trace_file	dmcl.ini	Replaced by new tracing implementation—refer to the *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* for information.
r_trace_level	dmcl.ini	Replaced by new tracing implementation—refer to the *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* for information.
client_cache_size	dmcl.ini	Implementation now allows per-session caches to dynamically adapt to free memory.
connect_timeout	dmcl.ini	Is specific to native code DMCL.
connect_recycle_interval	dmcl.ini	Is specific to native code DMCL.

Entry	Source	Comments
exception_count		Is specific to native code DMCL.
exception_count_interval		Is specific to native code DMCL.
terminate_on_exception		Is specific to native code DMCL.
i_override_list		
cache_queries		
max_connection_per_session		
use_local_always	dmcl.ini	Option to use server common area is not available in Foundation Java API 6.5, so this becomes unneeded.
use_local_on_copy	dmcl.ini	Option to use server common area is not available in Foundation Java API 6.5, so this becomes unneeded.

C.5 Obsolete dfc.properties keys

"Obsolete dfc.properties keys" on page 253 lists the `dfc.properties` keys that are obsolete since version 6.5. Setting these keys has no effect on Foundation Java API 7.x.

Table C-4: Obsolete dfc.properties keys

Entry	Source	Comments
dfc.tracing.combineDMCL	dfc.properties	Replaced by new tracing implementation—refer to the *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* for information.
dfc.tracing.compactMode	dfc.properties	Replaced by new tracing implementation—refer to the *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* for information.

Entry	Source	Comments
dfc.tracing.recordParameters	dfc.properties	Replaced by new tracing implementation—refer to the *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* for information.
dfc.tracing.recordReturnValue	dfc.properties	Replaced by new tracing implementation—refer to the *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* for information.