ORACLE®

PRIMAVERA

P6 EPPM Content Repository Configuration Guide
16 R2

September 2016

Contents

About Connecting the Content Repository

Having a content repository integrated with P6 can turn cluttered, unstructured content into organized assets by making it easier to catalog, access, search, and reuse documentation.

This guide will tell you how to:

- Configure Oracle Webcenter Content Core Capabilities (WCCC), Oracle Database, Microsoft SharePoint or any CMIS-compliant content repository when you install it. Refer to *Tested Configurations* for the full list of the content repositories and the versions that P6 EPPM supports.

  Notes:

  - The SharePoint connector is deprecated. The SharePoint connector is supported in this release, but might not be supported in a future release.

  New SharePoint users should configure SharePoint with a CMIS-compliant content repository, and then configure P6 EPPM to the CMIS-compliant content repository.

- Set your content repository settings in the Primavera P6 Administrator to connect your content repository to P6.

About Content Repository Authentication Modes

P6 EPPM offers two content repository authentication modes. You can configure authentication for either single user authentication or multiple user authentication. In single user authentication mode, all P6 EPPM users access the repository using a single administrator user login that is set during repository configuration. In multiple user authentication mode, each P6 EPPM user is authenticated based on their individual login.

Single User authentication mode is useful when you want users to have full access to the content repository through P6 EPPM without having to maintain an equivalent list of users for both P6 EPPM and the repository. This allows a repository administrator to maintain one set of credentials for the repository without having to share those credentials with all users. Single user authentication is also useful for quickly setting up test repositories that testers can access with ease.

Multiple User authentication mode is the default mode. Multiple user authentication mode provides increased security by restricting content repository access on an individual user basis. Because it uses native auditing fields it also allows a clear audit of who has created and modified files.

Note:

- When using multiple user authentication mode, you should disable for the Oracle content repository Guest Access. If you leave Guest Access enabled and the guest user is not part of the P6 EPPM security group, that user will not be able to access P6 repository functionality.
- If you are using the Oracle Database as your content repository, you can only use multiple user.

See the *P6 EPPM Application Administration Guide* for more information about Single User and Multiple User settings.

Configuring the Content Repository for P6

If you are installing P6 and the content repository for the first time, follow the steps in this section.

If you are upgrading from a previous version of P6 and need to update your content repository to the latest supported version, you need to follow the steps in ***Upgrading the Content Repository*** (on page 18).

Before you configure your content repository, you need to decide which authentication mode to use. Refer to the documentation included with the content repository application for detailed instructions on how to complete the guidelines in this section.

Note: When P6 is configured with a content repository, it develops a dependency on that content repository. After you configure your content repository, if dependency is broken (for example, starting P6 when the content repository is not running), the content repository features will fail until the P6 Server is restarted.

Configuring Oracle Webcenter Content Core Capabilities to Work with P6

Depending on your organization, you can choose to use existing configurations or your own naming conventions when configuring Oracle Webcenter Content Core Capabilities (WCCC). Refer to the documentation included with WCCC for detailed instructions on how to complete the guidelines in this section. See the *P6 EPPM Tested Configurations* document for information on supported versions.

These instructions contain information only on configuring Oracle Webcenter Content Core Capabilities to work with P6. They do not include information on installing WCCC. For WCCC installation instructions, see the documentation included with Oracle WCCC. For more information on configuring Oracle Webcenter Core Capablities, consult the following Knowledge Base article on integrating WCCC with P6:
https://support.oracle.com/epmos/faces/DocumentDisplay?id=2019531.1.

Configuring an Intradoc Server Port in WCCC

The Intradoc Server Port is used by P6 to communicate with WCCC. When this is enabled, a security filter list which includes the IP address of the P6 application server is required to communicate to the Content Server through the Intradoc Server Port. The security filter list must be defined because it is a trusted connection. If you are accessing WebContent Center for the first time, you must configure the Incoming Socket Connection Address Security Filter and Server Socket Port.

To configure the Incoming Socket Connection Address Security Filter and Server Socket Port:

1) Log in to WebCenter Content `(http://<host>:<port>/cs`) as an administrator. The default is weblogic.
2) Enter or edit the following configuration values:
   a. In **Incoming Socket Connection Address Security Filter**, enter the server IP address of the P6 application server.

      Note: Separate multiple IP addresses using a pipe symbol or |. For example, `127.0.0.1|127.0.0.2`.

   b. In **Server Socket Port**, enter an unused port number for the Content Server. For example, 4444.
3) Apply the changes.
4) Restart the WCCC managed server for changes to take effect.

   Note: If this is not the first time you have installed WCCC, you must confirm or modify the server configuration Incoming Socket Connection Address Security Filter and Server Socket Port values. You can modify the values through Enterprise Manager or with the configuration file (config.cfg) using the following procedures:

   - ***Modifying the Server Configuration through Enterprise Manager*** (on page 7)
   - ***Modifying the Server Configuration using the Configuration File*** (on page 8)

Modifying the Server Configuration through Enterprise Manager

To modify the server configuration through Enterprise Manager:

1) Connect to Enterprise Manager Fusion Middleware Control (`http://<server>:<port>/em`).
2) Log in as a domain administrative user. For example, weblogic.
3) In the navigation tree, expand **WebCenter, Content**, **Content Server**.
4) Select the Content Server instance name (for example, Oracle Content Server (WCCC_server1)).
5) Use the WCCC menu to select **Configuration Pages**, **Internet Configuration**.

6) In the Server Configuration section, in the **IP Address Filter** field, enter a list of IP addresses that can be used to access the server.

> **Note:** Separate multiple IP addresses or machine name entries using a pipe symbol or |. For example, `127.0.0.1|127.0.0.2`.

7) In the **Intradoc Server Port** field, enter a server port number.
8) Apply the changes.
9) Restart the WCCC managed server for changes to take effect.

Modifying the Server Configuration using the Configuration File

To edit the files in the server:

1) Go to <`WCCC_Home>\ucm\cs\config`. `WCCC_Home` is the location where you installed WCCC. The `WCCC_Home` path is `\Oracle\Middleware\user_projects\domains\$domain_name` by default.
2) Edit the config.cfg file.
3) Find the SocketHostAddressSecurityFilter line and add the list of IP addresses that can be used to access the server to the end of the line.

> **Note:** Separate multiple IP addresses or machine name entries using a pipe symbol or |. For example, `127.0.0.1|127.0.0.2`.

4) Find the IntradocServerPort line and enter a server port number. For example, 4444.
5) Save the changes.
6) Restart the WCCC managed server for changes to take effect.

Enabling Framework Folders in WCCC

The Framework folder interface is not enabled by default. See the WCCC documentation for more information.

To enable the Framework Folders component:

1) Log in to WebCenter Content `(http://<host>:<port>/cs`) as an administrator.
2) On the Main Menu, choose **Administration**, **Admin Server**, **Component Manager**.
3) On the Component Manager page, select the **FrameworkFolders** option.
4) Click **Update**.
5) Restart the WCCC managed server for changes to take effect.

Creating a P6 Security Group in WCCC

To maintain your WCCC repository, create a P6 Security Group in WCCC and grant the appropriate rights to P6 EPPM users. Consider the following:

- P6 user names must match the WCCC user names, unless you are using Single User for the Authentication Mode.

> **Note:** Single User Authentication Mode will log all P6 users into WCCC using the administrator user or as specified in the Database/Instance/Content Repository setting in P6 Admin Settings.

- All P6 EPPM-related WCCC user names must have corresponding assignments to WCCC Roles and Users. For a quick setup, you can create one P6 EPPM-specific Role to map to users with full privileges (read, write, delete, admin).
- All P6 EPPM-related WCCC user names must have access to the P6 Security Group, either directly or through a role.

When you are creating users in WCCC for integrating with P6, consider the following:

If you are using Multiple User Authentication Mode when configuring P6:

- You must create a WCCC user for every P6 EPPM user, and the user name created must match the P6 EPPM user.
- You must assign the user to a role mapped to the security group associated with the P6 Framework folder and must have the right to read, write, and delete.
- You must create an administrative user in WCCC. The user name does not have to match a P6 user.
- You must assign the administrative user to a role mapped to the Security Group associated with the P6 folder. The administrator must have read, write, delete, and admin rights within the Security Group.

If you are using Single User Authentication Mode when configuring P6:

- You must create an administrative user in WCCC. The user name does not have to match that of a P6 EPPM user.
- You must assign the administrative user to a role mapped to the Security Group associated with the P6 folder. The administrator must have read, write, delete, and admin rights within the Security Group.

(Optional) If you enabled Security Accounts, create a P6 Security Account. Depending on your organization, you might need to set up a Security Account for performance and storage reasons. Security considerations include the following:

- P6 EPPM user names must match the WCCC user names, unless using Single User for the Authentication Mode.
- All P6-related WCCC user names must have corresponding WCCC Roles and Users.
- All P6-related WCCC user names must have access to the P6 Security Account.

Creating a Local P6 Security Group in WCCC

To create a local P6 Security Group and administrative user:

1) Log in to WebCenter Content (`http://<host>:<port>/cs`) as an administrator.
2) Expand **Administration**, and select **Admin Applets**.
3) Select **User Admin**.
4) In the User Admin dialog box, select **Security**, **Permission by Group**.
5) Click **Add Group**.
6) Enter a Group Name and description.
7) Click **OK**.
8) Close the Permission by Group dialog box.
9) Select **Security**, **Permission by Role**.
10) Click **Add New Role**.
11) Enter a Role Name and Display Name.
12) Click **OK**.
13) Select newly created role and click **Edit applet Rights**.
14) Grant all rights to the administrative user.
15) Click **OK**.
16) In the Groups/Rights section, select the newly created group.
17) Click **Edit Permissions**.
18) Grant all permissions to the group.
19) Click **OK**.
20) Close the Permission by Role dialog box.
21) In the User Admin dialog, click **Add**.
22) Set Authorization type to **Local**.
23) Click **OK**.
24) Provide user details.
25) Navigate to the Roles tab.
26) Click **Add Role**.
27) Add the newly created role.
28) Click **OK**.
29) Close the User Admin dialog box.

Creating an External P6 Security Group in WCCC

You may want to create external security accounts for WCCC. For instructions on creating external security groups, see the document "How To Configure Local Or External Users, Roles And Security Accounts In Webcenter Content Core Capabilities (WCCC), Universal/Enterprise Content Server When Integrating With P6 EPPM" (Doc ID 2019531.1 on My Oracle Support at http://support.oracle.com.

Creating Document Types for P6 Documents in WCCC

(Optional) You can create document types for P6 documents in WCCC.

1) Log in to WebCenter Content `(http://<host>:<port>/cs)` as an administrator.
2) Expand **Administration** and select **Admin Applets**.
3) Select **Configuration Manager**.
4) In the Configuration Manager, select **Options**, **Content Types**.
5) Create a new content type for P6 Documents.
6) Apply the changes.
7) Restart the WCCC managed server for changes to take effect.

Note: Document Type as Document is the default document type in a WCCC repository.

Creating a P6 Documents Home Folder on the WCCC Server

Create a P6 documents home folder on the WCCC server by adding a unique path to the root folder.

1) Log in to WebCenter Content `(http://<host>:<port>/cs)` as an administrator.
2) Expand **Browse Content**.
3) Select **Folders**.
4) Select **Add**.
5) Enter a folder name. For example, P6EPPM
6) Select **Show Advanced Options**.
7) Select the security group created for P6.
8) Apply the changes.

Creating Metadata Text Fields in WCCC

From the Configuration Manager applet, create the following metadata text fields in WCCC for P6:

1) Log in to WebCenter Content `(http://<host>:<port>/cs)` as an administrator.
2) Expand **Administration** and select **Admin Applets**.
3) Select **Configuration Manager**.
4) In the Configuration Manager, select the **Information Fields** tab.
5) Create the following information fields as specified (including case):
    - PrmUserId
    - PrmProjectId
    - PrmWorkgroupId
    - PrmWorkflowId
    - PrmWorkflowStatus
    - PrmWorkflowAction

- PrmSecurityPolicy
- PrmTemplate
- PrmCheckedOutUserId
- PrmCheckedOutDate
- PrmLocalFilePath (set Type to **Long Text**)
- PrmAuthorId

> **Note:** Using "Prm" as a prefix is optional. You can use any prefix. If you do not use a prefix, ensure that none of the P6 metadata fields conflict with existing metadata fields.

6) Select **Update Database Design** to commit the changes.
7) Restart the WCCC managed server for changes to take effect.

Configuring WCCC settings for the Primavera P6 Administrator

To configure WCCC settings for the Primavera P6 Administrator:

1) Open the Primavera P6 Administrator.
2) In the Configurations tab, expand your configuration.
3) Expand **Database**, **Instance[n]** , **Content Repository**.
4) In the **Type** field, choose **Oracle**.
5) Expand **Database**, **Instance[n]**, **Content Repository**, **Oracle WebCenter Content Core Capabilities**.
6) In the **Host** field, enter the machine name or IP address of the content repository server.
7) In the **Port** field, enter the Intradoc Server Port number of the content repository server. The default port number is 4444.
8) In the **Oracle Home field**, enter the location of the folders you created. The default for Framework Folders is `/P6EPPM`.
9) In the **Oracle Security Group** field, enter the name of the Security Group for P6 documents that you specified when you configured the content repository.
10) In the **Oracle Security Account** field, enter the name of the Security Account for P6 documents that you specified when you configured the content repository. If you did not enable security accounts, leave this field blank.
11) In the **Oracle Document Type** field, enter the document type for P6 documents, which can be either an existing document type or a new one that you specified when you configured the content repository. If you enabled Document Types, you must configure this setting. For example, document.
12) In the **Metadata Prefix** field, enter the prefix added to P6 metadata fields, as specified when you configured the content repository. For example, Prm.
13) In the **Admin User** field, enter the user name with administrative privileges that you specified when you configured the content repository.
14) In the **Authentication Mode** field, enter the authentication mode that you use access the content repository server. For example, Single User or Multiple User. P6 EPPM users cannot access content repository functions if you do not configure this setting.

> **Note:** If you choose Multiple User, all P6 EPPM content repository-related user names must match the equivalent content repository user name. For example, a P6 EPPM user named "Joe" must have an equivalent user named "Joe" in the content repository.

15) Restart the P6 server.

Configuring CMIS-Compliant Content Repository for P6

Content Management Interoperability Services (CMIS) is a standard that content repositories have agreed to adhere to so that a single document connector can be used to connect to any CMIS-compliant repository.

You can connect any CMIS-compliant content repository, including SharePoint, to P6. The repository must be 100% CMIS-compliant to utilize all the features of P6 document functionality.

Configuring CMIS-Compliant Content Repository in the Database Instance Settings

You can use Microsoft SharePoint with P6 by integrating SharePoint with your CMIS-compliant content repository and then configuring your CMIS-compliant content repository with P6.

To configure your CMIS-compliant content repository:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Database/Instance[n]/Content Repository**.
4) In the **Type** field, choose **CMIS**.
5) In the **Maximum document size** field, enter the maximum size for documents that can be uploaded to P6. The default is 10240 KB. You can enter anything from 0-1048576 KB.
6) Expand **Database/Instance[n]/Content Repository/CMIS**.
7) In the **Login Name** field, enter the user name for your content repository.
8) In the **Password** field, enter the password for the user name you entered above.
9) In the **Authentication Mode** field, enter authentication mode used to access the content repository server. P6 EPPM users cannot access content repository functions if you do not configure this setting.

   If you choose "Multiple User", all P6 EPPM content repository-related user names must match the equivalent content repository user name. For example, a P6 EPPM user named "Joe" must have an equivalent user named "Joe" in the content repository.

   If you choose "Single User", the administrative user specified in the setting above must have access to all appropriate Security Groups to browse to documents outside of the P6 EPPM home folder.
10) In the **Repository Name** field, enter the name for your content repository.
11) In the **Document Home** field, enter the location of your documentation home where you want to store P6 documents.
12) In the **Web Service URL** field, enter the URL for your web services home.
13) Restart the P6 server.

Configuring AutoVue

There are two ways that you can configure AutoVue for use with P6 EPPM:

- **Configuring AutoVue without VueLink (global configuration):** Configuring AutoVue without VueLink is the native AutoVue implementation. To use this implementation, you will configure a single AutoVue server that is common across all database instances. For details, see ***Configuring AutoVue without VueLink*** (on page 14).
- **Configuring AutoVue with VueLink (individual configuration)**: Configuring AutoVue with VueLink supports VueLink integration for individual content repositories. To use this implementation, you will configure AutoVue for each individual database instance. For details, see ***Configuring AutoVue with VueLink*** (on page 15).

> **Note**: When upgrading to 16 R2 from 15 R2 or earlier, AutoVue connection details are lost and must be enter again.

Configuring AutoVue without VueLink

Configuring AutoVue without VueLink is the native AutoVue implementation. To use this implementation, you will configure a single AutoVue server that is common across all database instances.

> **Note**: When you configure AutoVue without VueLink, you are creating global AutoVue settings. These settings override any individual settings you may have created to configure AutoVue with VueLink. If you plan to configure AutoVue with VueLink, you must disable the global settings by setting the **Enable** field to **false**, as described in step 4 below.

To configure AutoVue without VueLink, complete the following steps:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **AutoVue**.
4) In the **Enable** field, set **true** or **false**. The default setting is **false**.

> **Notes:**
>
> - SSL mode does not work when the Enable option is set to false.
> - By default, the ESAPI resources that come with VueLink is used. You can change the location of the resource files by using `-Dorg.owasp.espai.resources JAVA_OPTIONS` in the WebLogic application server or in the *setDomainEnv* script.
> - By default, `dmsstamp.ini` and the oracle sample stamp from VueLink is used to create markup. You can change the location of the `dmsstamp.ini` file, which contains the stampfile location, using `-Dexternal.csi.intellistamp.def.location JAVA_OPTIONS` in the WebLogic application server or in the `setDomainEnv` script.

- If using Oracle Access Manager with your P6 EPPM deployment, add the context roots `/p6/VueServlet/**` and `/p6/jvueDMS/**` to the Oracle Access Manager exclusion list. For more information about protecting your resources using Oracle Access Manager's exclusion list, see the "Protecting Your Resources" chapter in the *Oracle Access Manager Configuration Guide*.

5) In the **Hostname** field, enter the hostname for the server where AutoVue is installed.

Note: Do not put a / at the end of the URL.

6) In the **Port** field, enter the port for the server where AutoVue is installed. The default port is **5099**.
7) Restart the P6 server.

Configuring AutoVue with VueLink

Configuring AutoVue with VueLink supports VueLink integration for individual content repositories. To use this implementation, you will configure AutoVue for each individual database instance.

Note: When you configure AutoVue with VueLink, you are creating individual AutoVue settings for each database instance. These settings are overridden by any global settings you may have created to configure AutoVue without VueLink. If you plan to configure AutoVue with VueLink, you must disable the global settings by setting the Enable field to false, as described in ***Configuring AutoVue without VueLink*** (on page 14).

To configure AutoVue with VueLink, complete the following steps:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Database/Instance[n]/Content Repository/AutoVue**.
4) In the **VueLink URL** field, enter the URL of the server hosting AutoVue VueLink.

   The default is `http://localhost:port/cs/idcplg?IdcService=VIEW_IN_AUTOVUE`.

Note: Do not put a / at the end of the URL.

In the **Enable** field, set **true** or **false**. The default setting is **false**.

5) Restart the P6 server.

Configuring Microsoft SharePoint to Work with P6

Refer to the documentation included with Microsoft SharePoint for detailed instructions on how to complete the steps in this section.

Notes:

- These instructions contain information only on configuring Microsoft SharePoint to work with P6. They do not include information on installing Microsoft SharePoint. For Microsoft SharePoint's installation instructions, see the documentation included with Microsoft SharePoint.
- Oracle recommends that you install the P6 SharePoint Connector on the same Internet Information Server (IIS) where you installed SharePoint. However, if you want to install it on a different server, you must install the P6 SharePoint Connector on an IIS where it can continually connect to the SharePoint server and Web Access Server in the same Local Area Network.

To configure Microsoft SharePoint:

1) Create a new site named "WS_FPRPC" (recommended name) on the Microsoft IIS using the IIS Admin.
2) If not already installed, install Microsoft .Net Framework 3.5 SP1. You can download it from this Web site: http://msdn.microsoft.com/en-us/netframework/cc378097.
3) From the **\Tools\SharePoint Connector** folder of the P6 EPPM physical media or download, launch **setup.exe** to install P6 EPPM Web Services on the "WS_FPRPC" site.
4) During the web service installation, retain the default virtual directory. For example, on the **Select Installation Address** dialog box, enter the following:

   Site = WSFPRPC
   Virtual Directory = WS_FPRPC
   Application Pool = DefaultAppPool
5) Once the installation finishes, test the installation by launching the following URL:

   http://*host*:*port*/*virtual_dir*/WS_FPRPC.asmx

   where *host* is the server machine name or IP address where you installed SharePoint, *port* is the port number that SharePoint is using (the default is 80), and *virtual dir* is the default virtual directory (for example, WS_FPRPC).
6) From the **\Tools\SharePoint Connector** folder of the P6 EPPM physical media or download, upload one of these templates to the SharePoint server:
   - For SharePoint 2010 or 2013, **WebAccessLibraryTemplate2010.stp**.
7) Go to **Site Actions**, **Site Settings**, **List Templates** and create a SharePoint document library for P6 EPPM. Note what you call the document library.
8) Enter the appropriate settings in the Primavera P6 Administrator. For more information, refer to ***Configuring Microsoft SharePoint in Primavera P6 Administrator*** (on page 17).

Note: You will configure the Primavera P6 Administrator settings when you run the P6 EPPM Configuration Wizard. See About the P6 EPPM Configuration Wizard.

Configuring Microsoft SharePoint in Primavera P6 Administrator

To set your SharePoint settings:

Note: Ensure the settings you entered in Troubleshooting the SharePoint connector match the settings you enter below.

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Database/Instance[n]/Content Repository**.
4) In the **Type** field, choose **SharePoint**.
5) In the **Maximum document size** field, enter the maximum size for documents that can be uploaded to P6. The default is 10240 KB. You can enter anything from 0-1048576 KB.
6) Expand **Database/Instance[n]/Content Repository/SharePoint**.
7) In the **Login Name** field, enter a SharePoint user name with administrative privileges.

   Note: You do not need to include your domain. You just need your user name.

8) In the **Password** field, enter the password for the SharePoint login name.
9) In the **Authentication Mode** field, select the mode used to connect to the SharePoint content repository database. P6 EPPM users cannot access content repository functions if you do not configure this setting.

   If you choose "Multiple User", all P6 EPPM content repository-related user names must match the equivalent SharePoint user name. For example, a P6 EPPM user named "Joe" must have an equivalent user named "Joe" in SharePoint.

   If you choose "Single User", the administrative user specified in the setting above must have access to all appropriate SharePoint libraries to browse to documents outside of the P6 EPPM home folder.

10) In the **Host Name** field, enter the machine name or IP address of the SharePoint server.
11) In the **Domain** field, enter the domain where the SharePoint server resides.
12) In the **Document Library URL** field, enter the URL of the P6 EPPM document library on SharePoint that you created when you configured SharePoint. The URL includes the machine name (or IP address) of the content repository server and the path to the content repository library.

    Example format:

    http://*<hostname>:<port>/<domain>/<doclib>*

    Note:

    - Do not put a / at the end of the URL.

- Ensure there are no spaces in the URL.

13) In the **Web Service URL** field, enter the URL of the Web Service used to connect P6 EPPM to SharePoint, as specified when you configured SharePoint. The URL includes the machine name (or IP address) of the content repository server, port number of the server, and web service name.

    Example format:

    http://*<hostname>:<port>/WS_FPRPC*

    Note: Do not put a / at the end of the URL.

14) In the **External Document Library URL** field, enter the URL of an external document library. If you need to connect to a non-P6 EPPM document library, you must configure this setting.

    Example format:

    http://*<hostname>:<port>/<extdoclib>*

15) Restart the P6 server.

Configuring the Oracle Database Content Repository

To configure the Oracle database as your content repository:

1) Open the Primavera P6 Administrator.
2) In the **Configurations** tab, expand your configuration.
3) Expand **Database/Instance[n]/Content Repository**.
4) In the **Type** field, choose **Oracle Database**.

   This option will save documents and associated information in the P6 database schema. This option is only applicable if you are using an Oracle database on-premises.

5) In the **Maximum document size** field, enter the maximum size for documents that can be uploaded to P6. The default is 10240 KB. You can enter anything from 0-1048576 KB.

   Note: Ensure that the **Enable Cloud Storage** field is set to **false**.

6) Restart the P6 server.

Upgrading the Content Repository

If you upgraded to P6 or the content repository, you need to do one of the following:

- If you upgraded from a previous P6 version, see ***Migrating the Content Repository if Upgrading*** (on page 19).
- If you upgraded UCM to 11.1.1.9 or higher, see ***Upgrading from Previous Universal Content Management Version to WCCC*** (on page 19).

Migrating the Content Repository if Upgrading

Run the migration utility before connecting the upgraded environment back to the Content Repository. Running the migration utility will ensure all project folder names in the Content Repository change from Database IDs to their Project ID field (from P6).

If you upgraded P6 from a previous version, you must:

1) Go to the **P6EPPM_Home/p6** folder.
2) Run **migrationtool.cmd** or **migrationtool.sh** (based on your operating system).

Upgrading from Previous Universal Content Management Version to WCCC

If you were using a previous version of Universal Content Management (UCM), you will notice many changes when you upgrade to a supported version of WCCC. To maintain your documents from P6, you should ensure that your framework folder has updated correctly. To do this, you should:

1) Shutdown all the P6 applications connecting to your current content repository.
2) Run the migration utility.
   a. Go to the **P6EPPM_Home/p6** folder.
   b. Run **migrationtool.cmd** or **migrationtool.sh** (based on your operating system).

   > **Note**: **Users** is a restricted folder name for folders within the folder structure in supported versions of WCCC.

3) Note the folder database converts project IDs to project short names.
4) Upgrade a previous version of UCM or WCCC to a supported version of WCCC or higher using the upgrade guide provided with the WCCC media packs.
   a. Enable the framework folders components.
5) After the migration:
   a. Locate the **migration_run****** folder that was created.
   b. Move all the folders and documents under this folder to the Content repository home folder that you want to use.
   c. Ensure you select **inhibit propagation** to ensure proper movement of documents and folders.
6) After the move completes, you can start using the documents with the correct content repository home.

Tips

- Have 4-6 GB open memory space.
- Don't propagate changes when given the option.

Troubleshooting

If you started using the document functionality of the P6 application without running migration utility provided with P6 on an upgraded environment, where you were using a content repository for managing documents, you will be unable to use the documents that were earlier associated with any Projects or Users.

Legal Notices

Oracle Primavera P6 EPPM Content Repository Configuration Guide

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are “commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software or hardware and documentation may provide access to or information on content, products and services from third-parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.