Kofax Communications Manager

Repository Administrator's Guide

Version: 5.4.0

Date: 2020-08-26

KOFAX

Table of Contents

Preface

This administrator's guide contains a description of common administrative tasks and configuration of the Repository for Kofax Communications Manager (KCM), a communication development and document management system.

Related documentation

The documentation set for Kofax Communications Manager is available here:[1]

https://docshield.kofax.com/Portal/Products/KCM/5.4.0-cli2a1c07m/KCM.htm

In addition to this guide, the documentation set includes the following items:

Kofax Communications Manager Release Notes
Contains late-breaking details and other information that is not available in your other Kofax Communications Manager documentation.

Kofax Communications Manager Technical Specifications
Provides information on supported operating system and other system requirement for Kofax Communications Manager.

Kofax Communications Manager Installation Guide
Contains instructions on installing and configuring Kofax Communications Manager and its components.

Kofax Communications Manager Getting Started Guide
Describes how to use Contract Manager to manage instances of Kofax Communications Manager.

Kofax Communications Manager Batch & Output Management Getting Started Guide
Describes how to start working with Batch & Output Management.

Kofax Communications Manager Repository User's Guide
Includes user instructions for Kofax Communications Manager Repository and Kofax Communications Manager Designer for Windows.

Help for Kofax Communications Manager Designer
Contains general information and instructions on using Kofax Communications Manager Designer, which is an authoring tool and content management system for Kofax Communications Manager.

[1] You must be connected to the Internet to access the full documentation set online. For access without an Internet connection, see "Offline documentation" in the Installation Guide.

Kofax Communications Manager Template Scripting Language Developer's Guide
Describes the KCM Template Script used in Master Templates.

Kofax Communications Manager Core Developer's Guide
Provides a general overview and integration information for Kofax Communications Manager Core.

Kofax Communications Manager Core Scripting Language Developer's Guide
Describes the KCM Core Script.

Kofax Communications Manager Batch & Output Management Developer's Guide
Describes the Batch & Output Management scripting language used in KCM Studio related scripts.

Kofax Communications Manager Repository Developer's Guide
Describes various features and APIs to integrate with Kofax Communications Manager Repository and Kofax Communications Manager Designer for Windows.

Kofax Communications Manager ComposerUI for ASP.NET Developer's Guide
Describes the structure and configuration of KCM ComposerUI for ASP.NET.

Kofax Communications Manager ComposerUI for J2EE Developer's Guide
Describes JSP pages and lists custom tugs defined by KCM ComposerUI for J2EE.

Kofax Communications Manager ComposerUI for ASP.NET and J2EE Customization Guide
Describes the customization options for KCM ComposerUI for ASP.NET and J2EE.

Kofax Communications Manager DID Developer's Guide
Provides information on the Database Interface Definitions (referred to as DIDs), which is a deprecated method to retrieve data from a database and send it to Kofax Communications Manager.

Kofax Communications Manager API Guide
Describes Contract Manager, which is the main entry point to Kofax Communications Manager.

Getting help with Kofax products

The Kofax Knowledge Base repository contains articles that are updated on a regular basis to keep you informed about Kofax products. We encourage you to use the Knowledge Base to obtain answers to your product questions.

To access the Kofax Knowledge Base, go to the Kofax website and select **Support** on the home page.

Note The Kofax Knowledge Base is optimized for use with Google Chrome, Mozilla Firefox or Microsoft Edge.

The Kofax Knowledge Base provides:

- Powerful search capabilities to help you quickly locate the information you need.

  Type your search terms or phrase into the **Search** box, and then click the search icon.
- Product information, configuration details and documentation, including release news.

  Scroll through the Kofax Knowledge Base home page to locate a product family. Then click a product family name to view a list of related articles. Please note that some product families require a valid Kofax Portal login to view related articles.
- Access to the Kofax Customer Portal (for eligible customers).

  Click the **Customer Support** link at the top of the page, and then click **Log in to the Customer Portal**.
- Access to the Kofax Partner Portal (for eligible partners).

  Click the **Partner Support** link at the top of the page, and then click **Log in to the Partner Portal**.
- Access to Kofax support commitments, lifecycle policies, electronic fulfillment details, and self-service tools.

  Scroll to the **General Support** section, click **Support Details**, and then select the appropriate tab.

Chapter 1

Administer KCM Repository

This chapter explains how to use the KCM Designer for Windows administrative interface, which is used to manage the KCM Repository installation.

Administrative account

KCM Repository has a built-in user account called ITP Admin, which is used for administrative purposes. The ITP Admin account has a number of advanced features:

- Enter and review KCM Repository licenses
- Manage active user sessions
- Manage user accounts and global user authorization
- Break locks on objects
- Set installation properties
- Remove deleted items from the database

ITP Admin account cannot perform common development tasks.

The ITP Admin account and its user sessions do not count against the number of users specified in the license. If a license violation occurs, you can use the ITP Admin account to resolve it.

Other users can be granted the "Allow login as Admin" right (for more information, see Create user accounts). The users with this right have the same rights as ITP Admin, without their standard advanced features. Such user sessions do not count against the license.

Note Versions prior to 4.2.1 do not support ITP Admin rights for other user accounts.

To log in as ITP Admin, follow these steps:

1. Start **KCM Designer for Windows**.
2. In the login dialog, enter the ITP Admin credentials and click **Login**.
   KCM Designer for Windows is opened.

To log in as administrator using a different account, follow these steps:

1. Start **KCM Designer for Windows**.
2. In the login dialog, enter your credentials and click **Login**.
   KCM Designer for Windows is opened.
3. On the menu, click **File** > **Log in as administrator** and enter the same credentials.

When the LDAP mode is enabled on the system, in the login dialog, select **Logon using One Time Token** and use a token generated in KCM Designer (for Web). To log in as administrator, on the KCM Designer for Windows menu, click **File** > **Log in as administrator**, generate another token in KCM Designer (for Web), and then use it in the login dialog. For more information on the token generation, see the Kofax KCM online Help.

Default password

The *itpadmin* user account has a default built-in password, which is *www.aia-itp.com*. For security reasons, KCM Repository forces you to change this password when you first log in as KCM Admin.

If the password to the KCM Admin account is lost, you can use another user account with administrative rights to reset the KCM Admin password.

If no user account is configured with administrative rights, you can use KCM Repository to regenerate the default password. To do so, you need access to the KCM Repository database and a tool to execute SQL commands against that database, as shown below.

1. Execute the following SQL statement. Place the statement on a new line.

   ```
   DELETE FROM T1200 WHERE C1201=1
   ```

   The statement removes the KCM Admin account.
2. Locate cvc.exe, which resides in the Programs folder of KCM Repository Server.
3. Restart KCM Repository Server and run cvc.exe within 10 seconds after starting the server.
4. Pass `/cfg=<path to the correct itprep.ini file for the instance such as <deploy root>\KCM\Work\<KCM version>\Instance_01\designer\Config\itprep.ini>` to cvc.exe to regenerate the KCM Admin account.
5. Once cvc.exe is finished, start KCM Designer for Windows, and then log in as KCM Admin with the default password.

   You are prompted to change the password.

After installation

The following section describes steps to perform after KCM Repository is installed, according to the instructions in the Kofax KCM Installation Guide.

Note The database attached to KCM Repository contains important production data. Make sure that you perform a database backup on a regular basis.

Enter licenses

1. Start KCM Designer for Windows.
2. Log in as ITP Admin (see Administrative account).
3. On the menu, click **View** > **License**.

   The **"License information"** window appears.

4. For the "ITP/MDK Repository base license," "ITP/MDK Repository model development license," and "ITP/MDK Repository textblock editing license," click **Edit**. The "DID development (SDK/MP) license" is only needed to develop DIDs in KCM Repository.

   The Model Development License and the Text Block Editing License come with a number of users. This is the number of user accounts and simultaneous user sessions that are allowed to develop Master Templates and edit Text Blocks, respectively.

   Note By default, the maximum storage size is 25 MB for Text Blocks, Master Templates, and other objects stored in the KCM Repository. To learn how to adjust this limit, see the section "Configure Tomcat settings" in the *Kofax Communications Manager API Guide*.

Administrative tasks

The following sections describe the tasks specific to ITP Admin or to users with administrative rights.

User management

Only the ITP Admin user or a user with administrative rights can create, delete or change user accounts. The user accounts reside in the Users folder. To learn how to create a user account, see Create user accounts.

Create user accounts

The KCM Admin account is intended for administrative purposes only. To participate in the development of Master Templates or perform other common KCM Repository tasks, you need to create one or more user accounts.

1. In the tree view, click **Users**.
2. On the menu, click **File** > **New User**.

   The **New User** window appears.
3. Enter a name, a full name, and a password, and then click **Add User**.

   A password must correspond to the password policy requirements. For more information on the requirements, see Configure the password policy.
4. At least one user account must have the right to create projects and assign roles to users. For more information, see Allow login as Admin right.

Allow login as Admin right

1. To allow the user to log in with the same rights as ITP Admin, in the tree view, click **Users**.
2. Right-click a user name in the right pane and then click **Configuration**.
3. To allow the user to log in with the same rights as ITP Admin, select the **Authorization** tab and select **Allow login as Admin**. When selected, the user can assign roles and create projects.
4. Click **OK**.

Unified logon

KCM Designer for Windows prompts the user to enter a name and password when starting. Optionally, the user may enter a Microsoft Windows account user name to log on to KCM Repository. This unified logon is performed automatically when KCM Designer for Windows is started. A verification is performed to ensure that the user name on the client is mapped to the same account on the server.

Note You cannot use unified logon when the LDAP mode is enabled in KCM Designer. For more information on LDAP, see User authentication in LDAP mode in this guide and the section "Authorize a user" in the Kofax KCM Designer online Help.

To use unified logon, create user accounts in KCM Repository with the names matching those for the Microsoft Windows user accounts. Also, KCM Repository Server must be configured to allow unified logon. To do so, add the following line to the itprep.ini file on the servers. The location of the itprep.ini files depends on the installation and the instance (see General).

```
[Configuration]
AllowUnifiedLogon=Y
```

When KCM Repository Server is configured to use unified logon, you can force KCM Designer for Windows to prompt the user to log in. To do so, start KCM Designer for Windows with the `/asklogin` flag or add the following line to the itprep.ini file of the clients.

```
[Configuration]
Asklogin=Y
```

If you are already logged on to KCM Designer for Windows, click **File** > **Switch user** to switch to another user.

Note If you switch to another user, your rights also change.

Rename a user account

1. In the tree view, click **Users**, and in the right pane, right-click the user name, and then click **Configuration**.
   The Configuration window appears.
2. In the **General** tab, change the login name and/or the full name of the user account.
   The user name has a maximum length of 254 characters. The full name has a maximum length of 79 characters.
3. Click **Apply** and click **OK**.

Authorize a user account

KCM Repository provides a role-based authorization functionality. A user can be assigned a role for all KCM Repository projects or for a specific project, folder or document. A role defines the actions a user is allowed to perform.

1. In the tree view, click **Users**, and in the right pane, select the user account.
2. Right-click the user account and click **Configuration**.
   The Configuration window appears.

3. In the **Authorization** tab, in the **Global roles** pane, select or deselect roles assigned to the user.
   To create new projects, at least one user must be assigned the Project Creator role.
4. Click **Apply** and click **OK**.

Note The roles assigned to a user account in the **"Global roles"** pane apply to all projects in KCM Repository. To assign roles for a specific project, folder or document, use the Configuration window for this project/folder/document.

Note When a new role is assigned to a user, the user must log out and then log in.

Reset a password

The Administrator can reset the user's password if it is lost. After a password change, the user's sessions will be ended. Ensure that the user has saved all changes before continuing.

1. In the tree view, click **Users**, and in the right pane, select the user account.
2. Right-click the user account and click **Change user password**.
   The **"Change the user password"** window appears.
3. Enter and repeat the new password and click **OK**.

Delete a user account

After a user account is deleted, the user's session will be ended. Ensure that the user has saved all changes before continuing.

1. In the tree view, click **Users**, and in the right pane, select the user account.
2. Right-click the user account, click **Delete**, and then click **Yes** to confirm the action.
   This user account can no longer be used to log on to KCM Repository. Also, the user account no longer counts against the maximum number of users in the license. To see objects created with this user account, click **View** on the menu, and then click **Show deleted items**.

Manage user sessions

To view and manage user sessions that are currently active:

1. On the menu, click **View** > **The Sessions**.
   The **"Active sessions"** window appears.
2. Click a user session and click **Refresh** or **Disconnect** to refresh or close the session, respectively.

User authentication in LDAP mode

When the LDAP mode is enabled, you can organize user accounts in LDAP groups and associate the groups with a role or a set of roles in KCM Designer.

To enable the mode for KCM Designer, follow the procedure described in the section "Enable LDAP mode for KCM Designer" in the *Kofax Communications Manager Getting Started Guide*.

Note
- When the LDAP mode is enabled, you cannot create or modify user accounts.
- When you switch from the non-LDAP to LDAP mode, ensure that no objects that are not shown in KCM Designer for Windows, such as Libraries or Resources, are left with status [in development]. In the LDAP mode, you cannot break lock on such objects.
- The Authorization tab in the Configuration window is not available in the LDAP mode.

Configure the password policy

ITP Admin, or other user who manages KCM installation, can shape the password policy. This can be done through configuration options in the itprep.ini file of the KCM Repository server of the instance.

Requirements for password

A password must meet the following requirements in a standard configuration. These requirements are enforced when changing a password.

- Be at least 12 characters long
- If less than 20 characters long, it should contain at least three of the following character types: lowercase letters, uppercase letters, digits, and other (symbols, punctuation, and so on)
- For languages without lowercase/uppercase distinction, all three following character types should be present: letters, digits, and other (symbols, punctuation, and so on)
- Not be used earlier by this user in the previous 12 months
- Additionally, if the organization has a list with forbidden passwords, the password should not be on this list. For information on how to configure a list of forbidden passwords, see Configure a list of forbidden passwords.

You can configure the two password lengths (12 and 20 by default) and the retention period for old passwords. For more information, see Adjust the password policy settings.

Note When an incorrect password is provided the user account will be locked out for five consecutive times at login. To unlock it, the administrator has to reset the password of this user account. For more information on how to reset a user's password, see Reset a password.

Adjust the password policy settings

Open the itprep.ini file and adjust the following settings, if necessary.

All values given in the following examples represent the default values.

1. **Password length settings**
   You can change the minimum acceptable length of a password with the `MinPasswordLength` setting.

   ```
   [Security]
   ```

```
MinPasswordLength=12
```

With the `MinSafePasswordLength` setting you can define the minimum password length for which the requirement of three different characters types is omitted.

```
[Security]
MinSafePasswordLength=20
```

If `MinSafePasswordLength` is set to `0`, all passwords require three different character types regardless of their length. If this setting is set to a value less than or equal to `MinPasswordLength`, passwords that satisfy the minimal length requirement do not need three different character types.

Example 1

```
[Security]
MinPasswordLength=12
MinSafePasswordLength=20
```

This example allows "a really long password" (22 characters) and "TestPassw0rd" (12 characters, 3 character types) but does not allow "testpassword" (12 characters, 1 character type).

Example 2

```
[Security]
MinPasswordLength=12
MinSafePasswordLength=0
```

This example allows "TestPassw0rd" (12 characters, 3 character types) but does not allow "testpassword" (12 characters, 1 character type) and "a really long password" (24 characters, 1 character type).

Example 3

```
[Security]
MinPasswordLength=12
MinSafePasswordLength=12
```

This example allows "a really long password" (24 characters), "TestPassw0rd" (12 characters, 3 character types), and "testpassword" (12 characters, 1 character type).

2. **Password reuse setting**

   With the `PasswordReuseAge` setting, you can configure the number of months that an old password is retained and forbidden to be reused.

   ```
   [Security]
   PasswordReuseAge=12
   ```

   If `PasswordReuseAge` is set to 0, it disables password reuse memory.

3. **Lockout count setting**

   With the `MaxFailedLogins` setting you can configure the number of times a user can provide wrong password before the user's account is locked out. If `MaxFailedLogins` is set to 0, the user account is never locked out due to providing the wrong password.

   ```
   [Security]
   MaxFailedLogins=5
   ```

4. **Failed logon delay setting**

   When a logon attempt fails, there is a waiting period measured in seconds before it can be attempted again. You can configure this waiting period with the `FailedLoginDelay`.The value of `FailedLoginDelay` should be at least 0 and at most 15.

   ```
   [Security]
   FailedLoginDelay=3
   ```

Note Restart the KCM Repository Server and Content Management API after changing these settings in the itprep.ini file.

Configure a list of forbidden passwords

To prevent use of common passwords, the administrator can configure a list of passwords that will be rejected as a new password for a user.

1. Create a .txt file with forbidden passwords, placing each password on its own line, or download such a list from the Internet.
2. Name the file pwdblacklist.txt. The file must be in UTF-8 format with a Byte Order Mark.
3. Place the file in the KCM Repository configuration directory: `<deploy root>\KCM\Work\<version number>\Instance_<instance number>\designer\Config`
   Example `C:\KCM\Work\5.4\Instance_01\designer\Config`
   The file pwdblacklist.txt may already exist. In that case, append your own list of passwords to the file.

   Note The case of the blacklisted passwords is not relevant: "password" in the blacklist will also block "Password", "PASSWORD", and "PassWord."

Note Restart the KCM Repository Server after changing this file. A very large list of forbidden passwords may cause the first login and changing passwords to slow down after restart.

Project management

This section describes project management functions that may be useful to administrators.

Break locks on objects

The Administrator can break locks on objects locked by users. The Administrator can both break a lock on a specific object or break all locks made by a user.

1. To break a lock on a specific object, in the tree view, locate and right-click the object, and then click **Break lock**.
   - If the Administrator is breaking a lock on a folder or a project, the **"Break lock"** window appears. Select the user who locked the folder/project and click **OK**. All objects belonging to the folder are now unlocked.
2. To break all locks made by a user, in the tree view, click **Users**.
3. In the right pane, right-click the user account, and then click **Break lock**.
   All objects in KCM Repository that are locked by this user are now unlocked.

Purge deleted items

To permanently remove objects that are marked as deleted, the Administrator can use the Purge function.

The function may not remove all objects marked for deletion. For example, when a user deletes a source document and does not delete the Master Template that was created based on it, the source document is

not purged until the Master Template is deleted as well. You cannot restore items once they are removed using the Purge function.

Also, the Administrator has a subfolder called "purging blocked by" that lists objects that prevent the revision from being removed. It may be used by these objects or configured in them (in case of folders and projects). The Administrator can see this subfolder under the revisions and base objects marked for deletion. The Show Deleted Items option must be enabled. To enable it, on the menu, click **View** and click **Show Deleted Items**.

A document revision takes up the same amount of disk space as the original document. If you delete and purge a revision, it is removed from the database and frees up disk space.

To purge an item, click it, and then click **File** > **Purge**.

View an audit log

The Administrator can view the Audit Log Entries to track important activities.

To view the Audit Log Entries, in the tree view, click **Audit Log Entries** and see the right pane.

Obtain a report

The Administrator can obtain reports on the contents of KCM Repository. The reports are implemented as Master Templates. Several predefined reports are available in the Reports project. You can create your own reports so they appear in the Reports when you open a new KCM Designer for Windows browser window.

1. To get a report when logged in as ITP Admin, in the tree view, click **Users**.
2. In the right pane, click the user account.
3. On the menu, click **Report**, and then click **User authorization**.

Clear a project

To free up disk space, the Administrator can perform a cleanup. The cleanup deletes labels and redundant versions of the documents used in a project. Versions are considered redundant if they have no status or are not in use. When the cleanup is complete, the document versions are marked for deletion and can be restored, but labels are removed permanently. To remove the document versions completely, use the Purge function (for more information, see Purge deleted items).

You should back up your data before performing a cleanup.

To perform a cleanup, click the project and, on the menu, click **Cleanup a Project**.

Administrator tools

This section gives a description of the tools that are available to the Administrator.

Dumping and loading the Repository database

You can dump the entire contents of the KCM Repository database to a file with the repdump tool. Later, this file can be read into a database with the reload tool.

The reload tool can load dump files from a KCM Repository installation version 5.2 and later. For versions previous to 5.2, you must use the same reload as the version used to create the dump.

The reload and repdump tools must be run under the same account as the KCM Repository Server. If this is not possible, you can supply the correct database password for the tools using the parameter `/dbpwd=<password>`.

```
Repdump /cfg=<path-to-config> "path\database dumpfile name" [/dbpwd=<password>]
```

```
Reload /cfg=<path-to-config> "path\dumped file name" [/cleardatabase] [/
dbpwd=<password>]
```

In `cfg=`, pass the tool the correct itprep.ini file for the instance such as `C:\KCM\Work\<KCM version>\Instance_01\designer\Config\itprep.ini`.

In `dbpwd=`, pass the database password necessary to connect to the KCM Repository database.

Note If you change the database password to a plain text in the itprep.ini, the password will be encrypted once connected to the database (see [ODBC]). If you do so for the repdump tool or reload tool, the password of the account your tool is running under will be encrypted. In case it is a different account than KCM Repository is running under, it might prevent KCM Repository from decrypting the password again if you use the same itprep.ini.

After loading the contents of a previous version, you need to upgrade the database to the current version.

1. Locate cvc.exe, which resides in the Programs folder of KCM Repository Server.
2. Restart KCM Repository Server and run cvc.exe.

You must run repdump.exe and reload.exe on the server that runs KCM Repository. Both tools are installed in the root of the KCM Repository Server installation. The repdump tool creates a Repdump.log, which resides in the same folder as the tool.

1. To use reload.exe, create a new database or select an existing database that can be emptied and refilled.
2. To load a file, stop KCM Repository. To do so, stop the KCM Repository service.

If you use an existing database, use the `/cleardatabase` flag to empty the database. You cannot add the content of a database dump file to the content of an existing KCM Repository database.

Note The `/cleardatabase` flag destroys all content in the database of the loading KCM Repository. Use it with caution.

The reload and repdump tools can be used together to migrate the KCM Repository database to another DBMS.

New database

You can create a new database for KCM Repository and a connection string to connect to it.

Note The database attached to KCM Repository contains important production data. Make sure to make a backup of the database on a regular basis.

Configure the new database

The new database must be configured on KCM Repository Server.

1. To configure the new database, navigate to the itprep.ini file and open it in a text editor such as Notepad.
2. Locate the following entry.

```
[ODBC]
ConnString=<connection string>
user=<db user>
password=<db user password>
```

3. Change the values after the equals sign. Provide a connection string for the new database after `ConnString=`. Also, change the database user name and password if necessary.

   Restart the server after changing the configuration file.

Initialize the new database and upload reports

Use cvc.exe to prepare the database and upload the Reports.

1. Start a command line prompt.
2. Change the folder to the folder where you installed the KCM Repository Server.
3. Execute the following command.

```
cvc reportsdump /cfg=<path to itprep.inifile>
```

   Note You can only see reports if one of your roles is allowed access to it. If you cannot see any reports, or you can see only some reports, check your authorization.

   Now you can open the client and start working with the new database.

Undo Publish

This section gives information about the Undo Publish feature that can be used to restore a previous set of published revisions. This can be useful in cases where the business application is rolled back to a previous version, and the documents must match it. Also, the feature can be used to return to the previous saved publication state when errors appear to be published in the current saved publication state.

Perform the Undo Publish operation

To perform Undo Publish, start the Windows PowerShell command prompt and use the following scripts that reside in `<deploy root>\Programs\<KCM version>\Management`:

- RollbackPublication.ps1
- ListPublications.ps1
- PurgePublications.ps1

Configure Undo Publish

You must configure Undo Publish to make it available. The configuration setting is located in the itprep.ini file for KCM Repository Server (on the typical location for itprep.ini, see General).

The following setting indicates how long a published revision is retained after it is replaced with a newer revision.

```
[Configuration]
MaxUndoPublicationDays=30
```

Also, this setting controls whether the feature is active or inactive. If `MaxUndoPublicationDays=` is omitted or set to 0, no publication states are saved.

Note After configuring `MaxUndoPublicationDays=`, restart the KCM Repository Server and the Content Management API.

After you configure the Undo Publish feature, the first publication creates the first saved publication state you can roll back to. Also, every action that creates a project, such as Import or Duplicate, generates an initial saved publication state for that project.

Restore a saved publication state

When an object, a Changeset or a set of objects gets the published status, KCM Repository records all published revisions in a project after another publication is performed. Every new publication produces another saved publication state.

Old saved publication states are discarded when more recent publications appear. For more information on the publication states validity period, see Configure Undo Publish.

You can restore only the publication that precedes the current one. To roll back to older saved publication states, repeat the action until the desired saved publication state is restored. You cannot undo a rollback.

Use RollbackPublication.ps1 to perform a rollback. Start the Windows PowerShell command prompt and execute the script.

The script has the following parameters:

- `Instance!Number` *Required*. Instance number the script should operate on.
- `Repository!User` Only required when the LDAP mode is disabled. User account in KCM Designer. This account needs the authorization to perform the Publish action on the project.

- `Repository!Password` Only required when the LDAP mode is disabled. Password for the KCM Designer user account.
- `Repository!Token` Only required when the LDAP mode is enabled. Logon token generated with KCM Designer. For more information, see KCM Designer online Help.
- `Repository!Project` *Required*. Name of the project with the last saved publication state to roll back to.
- `Action!Perform` *Optional*. If set to true, the rollback is performed. If omitted or set to another value, the actions that the rollback would perform are shown, but not executed.

Example 1: LDAP mode is disabled

```
RollbackPublication.ps1 Instance!Number=1
Repository!User=administrator Repository!Password=******
Repository!Project=InstallationTest Action!Perform=true
```

Example 2: LDAP mode is enabled

```
RollbackPublication.ps1 Instance!Number=1
Repository!Token=1n2Z58JX...
Repository!Project=InstallationTest Action!Perform=true
```

Publication states list

Use ListPublications.ps1 to list the saved publication states for one or all projects. Start the Windows PowerShell command prompt and execute the script.

The script has the following parameters:

- `Instance!Number` *Required*. Instance number the script should operate on.
- `Repository!User` Only required when the LDAP mode is disabled. User account in KCM Designer. This account needs no special authorization.
- `Repository!Password` Only required when the LDAP mode is disabled. Password for the KCM Designer user account.
- `Repository!Token` Only required when the LDAP mode is enabled. Logon token generated with KCM Designer. For more information, see KCM Designer online Help.
- `Repository!Project` *Optional*. Name of the project with the saved publication states to list. If omitted, the saved publication states for all projects are listed.

Example 1: LDAP mode is disabled

```
ListPublications.ps1 Instance!Number=1
Repository!User=administrator Repository!Password=******
Repository!Project=InstallationTest
```

Example 2: LDAP mode is enabled

```
ListPublications.ps1 Instance!Number=1
Repository!Token=1n2Z58JX...
Repository!Project=InstallationTest
```

The list is chronologically ordered and shows the difference between the saved publication state and the current publication state with the following markings:

- The `[cur]` marking indicates the current published state.
- The `[prv]` marking signifies the previous published state.

Also, the list also shows the date and time a saved publication state was created, the user who performed the publish action, and the date and time it was superseded by a newer saved publication state.

Publication state cleanup

When a publication is performed, KCM Repository automatically removes all saved publication states that have been superseded before the configured threshold.

To perform a cleanup of old saved publication states without creating a new publication, such as in cases when the system becomes inactive, you can manually trigger the cleanup using the PurgePublications script. Start the Windows PowerShell command prompt and execute PurgePublications.ps1.

The script has the following parameters:

- `Instance!Number` *Required*. Instance number the script should operate on.
- `Repository!User` Only required when the LDAP mode is disabled. User account in KCM Designer. This account needs no special authorization.
- `Repository!Password` Only required when the LDAP mode is disabled. Password for the KCM Designer user account.
- `Repository!Token` Only required when the LDAP mode is enabled. Logon token generated with KCM Designer. For more information, see KCM Designer online Help.
- `Action!Perform` *Optional*. if set to true, the cleanup is performed. If omitted or set to another value, the actions that the cleanup would perform are shown, but not executed.

Example 1: LDAP mode is disabled

```
PurgePublications.ps1 Instance!Number=1
Repository!User=administrator Repository!Password=******
Action!Perform=true
```

Example 2: LDAP mode is enabled

```
PurgePublications.ps1 Instance!Number=1
Repository!Token=1n2Z58JX...
Action!Perform=true
```

Privileges for other roles

The following sections describe role privileges that were not covered in the previous sections.

Configuration privilege

Use this privilege to edit the objects configuration. It gives access to the Configuration window for an object. With this privilege, a user can make changes to the name and the description of an object. The next privileges determine which of the other tabs of the Configuration window are shown. The General tab is hidden to users who have no privilege to edit the tab.

The Configuration privilege is needed to configure authorization, auto-includes, characteristics, DID/CC, Field Set, and project privileges.

Privilege to configure the Authorization tab

Use this privilege to assign and revoke roles. With this privilege, a user sees the Authorization tab in the Configuration window. The Authorization tab is hidden to users who have no privilege to edit the tab.

Privilege to configure the Field Set tab

Use this privilege to add and remove Field Sets from a Forms or Text Block folder. When a Forms folder is concerned, this privilege is also used to add and remove Text Block Lists from a Forms folder.

Privilege to configure the Characteristics tab

Use this privilege to set characteristics for a project. With this privilege, a user sees the Characteristics tab in the Configuration window. The Characteristics tab is hidden to users who have no privilege to edit the tab.

Privilege to configure the DID/CC and Style Documents tabs

Use this privilege to set the DID and Connection Configuration for a project or a folder as well as a Style Document. With this privilege, a user sees the tabs DID/CC and Style Document in the Configuration window of a project or a folder.

The DID/CC and Style Document tabs are hidden to users who have no privilege to edit these tabs.

Privilege to configure the Project tab

This setting is a privilege to configure a project. With this privilege, a user sees the Project tab in the Configuration window. The Project tab is hidden to users who have no privilege to edit the tab.

Chapter 2

Configuration

This chapter describes configuration issues.

General

Both KCM Designer for Windows and KCM Repository Server use itprep.ini configuration files. The files use the same syntax but have different content and settings. You can edit the .ini files in a text editor such as Notepad.

One itprep.ini file exists per server, and another exists for each client.

Typically, the file can be found in `<deploy root>\KCM\Work\<version number>\Instance_<instance number>\designer\Config`.

Example `C:\KCM\Work\5.4\Instance_01\designer\Config`

Note The configuration files are read only at startup. You need to restart KCM Designer for Windows on the client once you edit the client configuration file. Restart KCM Repository Server once you edit the server configuration file.

Syntax

Initialization file sections

Options and settings are arranged in sections in the configuration file. A section starts with the section name in square brackets on a separate line.

```
[Configuration]
```

Settings are added in "Name=value" format.

Note If a setting is not listed in the .ini file, it is set to the default value.

You can use a semicolon to comment out a line in the configuration file. It must be the first character on a line.

Shared configuration

The following configuration options are valid for both the client and the server.

[Configuration]

This example shows the "Set logging" options.

```
logfile = itprep.log
logsize = 10485760
logrotate = 10
```

Relevant information is recorded to a file specified by the log file settings.

You can use the `logrotate` setting to determine how many obsolete log files should be kept (renamed to itprep.log.1, itprep.log.2, and so on). A new log file is created every time KCM Repository starts, or when the size of the log file exceeds the value in bytes set with the `logsize` setting.

The following is the folder where temporary files are placed.

```
temppath = %TMP%
```

Defaults to the temp folder are specified by Microsoft Windows. You can specify another path. Sufficient disk space must be allocated for the temp folder.

Server configuration

All required settings are configured during installation. To edit the configuration file, navigate to the Programs folder on the Windows Start menu, find the KCM Repository Server folder, and then locate the Edit Configuration entry. This entry gives you access to the server configuration file.

Restart KCM Repository Server after editing the .ini file.

[Server]

In this section, the port number used by the server for requests is set. 2586 is the default value. Any port number below 65536 is valid.

```
[Server]
port=2586
host=<server name or IP address>
```

The `host` value is added to the configuration file by the installer from other KCM programs that use the same configuration file.

Unified logon

The following setting allows the user to log on to KCM Designer using the user's Microsoft Windows user account name.

```
[Configuration]
AllowUnifiedLogon=Y
```

Licenses

There are three following license sections: [Base license], [Model development license], and [Text Block development license]. Normally, these licenses are to be filled using KCM Designer for Windows. For more information, see Enter licenses.

The following keys occur for each of the three license sections. The values are provided on the license certificate. You must copy them.

```
company=
certificate=
environment=
date=
users=
key=
```

The `date=` value is the expiration date for the license given on the license certificate. Format: `yyyymmdd`.

The `users=` setting defines the maximum number of users that can be created and connected to the server. This number is on the license certificate. The Administrator is not considered as a user in terms of the license. For the base license, this value is 1.

[ODBC]

In the [ODBC] section, the connection with the database is configured. The Connection String entry is set during installation.

```
connString = <connection string>
```

The connection string specifies the ODBC driver to use, the database to connect to, and various database options.

Also, you can provide a data source name to store KCM Repository data.

```
DSN = <data source name>
```

In the following example, the user and password are provided as separate settings. They do not need to be included in the connection string. This allows the encryption of the password in the configuration file.

```
user = <user to connect to the ODBC DSN>
password = <password to connect to the ODBC DSN>
```

If the password is present in the configuration file in plain text, it is encrypted once a connection with the database is created. You can recognize the encrypted password by its `encrypted:` prefix. To change the database password in the configuration file, replace the `encrypted:` string with a new plain text password.

Note The user account used to access the DBMS must be configured so that its password does not expire, especially because it affects client access.

[Network]

Use the [Network] setting to reduce the size of the packages sent over the network. You can use this setting when network load errors occur.

```
msgsize= <packet size in kilobytes>
```

If network load errors occur, you should start with a package size of 64 KB. if the problems still occur, use packages of 32 or 16 KB in size, and so on. The default packet size limit is 512 KB.

Note Add the [Network] setting to any client connecting to a KCM Repository Server with an edited .ini file.

Restart the KCM Repository Server after editing the .ini file.

Timeouts

The time that it takes KCM Repository to analyze documents and compile Master Templates is limited to 60 seconds and 900 seconds, respectively. Large and complex documents may encounter a timeout. These limits can be configured in the itprep.ini file of KCM Repository Server.

```
[ITP]
ConversionTimeout=60
CompilationTimeout=900
```

The values shown above are default values.

If you encounter the message `crtmdl timed out`, increment the `CompilationTimeout` value.

If you encounter the messages `idoc2unc timed out`, `Generation timed out` or `Analysis timed out`, you should increment the `ConversionTimeout` value.

Restart KCM Repository Server to activate the changes.

Client configuration

All required settings are configured during installation. Restart KCM Designer for Windows after editing the .ini file.

[server]

The [server] section contains the settings used to connect to the KCM Repository Server host and port.

```
[Configuration]
port=2586
host=<server name or IP address>
```

The default value for `host` is localhost. It indicates the computer that KCM Repository Server runs on.

`Port` is the TCP/IP port number used to send requests to the Server. This port number should match the `port` value set in the [server] setting of the KCM Repository Server .ini file.

Chapter 3

Batch & Output Management metadata

You can manage the Batch & Output Management metadata loaded into a KCM Repository instance using the following PowerShell scripts, with one per management task:

- LoadOutputManagementMetadata.ps1
- SaveOutputManagementMetadata.ps1
- ClearOutputManagementMetadata.ps1
- CheckOutputManagementMetadata.ps1

All scripts require the following standard parameters.

Parameter	Description
`Instance!Number`	Required. Specifies the number of the instance for which the management task should be applied.
`Repository!User`	Only required when the LDAP mode is disabled. Specifies the name of a KCM Repository user with the "Allow login as Admin" right.
`Repository!Password`	Only required when the LDAP mode is disabled. Specifies the password of the KCM Repository user.
`Repository!Token`	Only required when the LDAP mode is enabled. Specifies the logon token generated with KCM Designer. For more information, see KCM Designer online Help.
`Report!File`	Optional. Specifies the name of the report file written by the management action. The use of this file depends on the specific task, as described in this chapter. If omitted, the default value is `output-management-metadata-report.txt`. **Note** If the path or file name given in this parameter already exists, it is overwritten.

To execute one of the scripts, do the following:

1. Start a PowerShell prompt.
2. Navigate to: `<Deploy Root>\KCM\Programs\<VersionNumber>\Management`
   Example `C:\KCM\Programs\5.4\Management`
3. Execute the script.

Load Batch & Output Management metadata

You can load the metadata into KCM Repository using the script LoadOutputManagementMetadata.ps1.

Prior to loading the metadata, export the metadata XML file from a Batch & Output Management installation. To do so, in KCM Studio, select the Administration tab, click **Configuration export** and then select the location to export the XML file.

In the script, the following parameter is added to the standard parameters.

Parameter	Description
`Source!Path`	Path to the metadata XML file to load.

Execute the following command, adding the actual parameter values.

```
.\LoadOutputManagementMetadata.ps1 Instance!Number=1 Repository!User=<username>
Repository!Password=<password> Source!Path=<metadata filepath> [Report!File=<report
 filename>]
```

The report file written by this script contains a list of Document Pack Templates that refer to Batch & Output Management metadata that no longer exists in the newly loaded metadata.

Save Batch & Output Management metadata

You can save the metadata using the SaveOutputManagementMetadata.ps1 script. Saving the metadata retrieves the stored values from KCM Repository and saves them to disk.

In the script, the following parameter is added to the standard parameters.

Parameter	Description
`Destination!Path`	Path to a file where the retrieved metadata will be stored. If no metadata is present, the file is not written. **Note** If the path or file name given in this parameter already exists, it is overwritten.

Execute the following command, adding the actual parameter values.

```
.\SaveOutputManagementMetadata.ps1 Instance!Number=1 Repository!User=<username>
Repository!Password=<password> Destination!Path=<metadata destination path> [Report!
File=<report filename>]
```

The report file written by this script returns information on whether the metadata is retrieved successfully.

Clear Batch & Output Management metadata

You can clear all Batch & Output Management metadata from KCM Repository using the script ClearOutputManagementMetadata.ps1.

The script only requires the standard parameters.

Execute the following command, adding the actual parameter values.

```
.\ClearOutputManagementMetadata.ps1 Instance!Number=1 Repository!User=<username>
Repository!Password=<password> [Report!File=<report filename>]
```

The report file written by this script contains a list of Document Pack Templates that refer to Batch & Output Management metadata. If no such Document Pack Templates exist, the report file returns information that the metadata is cleared successfully.

Check Batch & Output Management metadata

You can check for Document Pack Templates that use non-existent Batch & Output Management metadata.

The script only requires the standard parameters.

Execute the following command, adding the actual parameter values.

```
.\CheckOutputManagementMetadata.ps1 Instance!Number=1 Repository!User=<username>
Repository!Password=<password> [Report!File=<report filename>]
```

The report file written by this script contains a list of Document Pack Templates that refer to Batch & Output Management metadata that no longer exists in the currently loaded metadata.