IBM Case Manager
Version 5.3.1

Designing and Deploying Solutions Guide

SC19-3683-07

IBM Case Manager
Version 5.3.1

Designing and Deploying Solutions Guide

SC19-3683-07

Note
Before using this information and the product it supports, read the information in "Notices" on page 425.

This edition applies to Version 5 Release 3 Modification 1 of IBM Case Manager (product number 5725-A15) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Troubleshooting Case Manager Client 231

Accessibility features of IBM Case Manager

IBM® Case Manager includes features that make it more accessible for people with disabilities.

Important: The accessibility features are supported on Windows operating systems and Mozilla Firefox browsers only.

Keyboard input and navigation

Keyboard input
You can use the keyboard instead of a mouse to operate the product. To use any button on the user interface, move the focus to the button and press the spacebar or the Enter key.

Keyboard focus
The position of the keyboard focus is outlined to indicate which area of the window is active and where your keystrokes will take effect.

Response time adjustments
After 30 minutes of inactivity, the IBM Case Manager web client displays a time-out warning. You can adjust response times in the Session management pane of the WebSphere® Application Server administrative console.

Silent installation
For an accessible version of the installation, you must use the silent installation feature from the command line interface.

Configuration tool
For an accessible version of the IBM Case Manager configuration tool, you must use the command-line interface.

Keyboard shortcuts

You can use the keyboard to access all of the functions of IBM Case Manager.

In general, keyboard access conforms to standard Microsoft Windows guidelines.

Keyboard access differs from standard Microsoft Windows guidelines in the following ways:

Access keys, Tab key, and tables
Access keys are provided only for buttons and menu items. Press the Tab key to reach all fields.

Press the Tab key to move the cursor into a table and then use the arrow keys to move between cells. To move the cursor out of the table to the next field, press Tab. When the cursor is in a table, pressing Enter is not equivalent to clicking **OK** to close the window. You must move the cursor out of the table first.

You can switch between tabs by using the Left and Right Arrow keys when the focus is on the tab label itself. Otherwise, you can use CTRL+Tab to move to the next tab in sequence.

Case Manager Client context

Press Alt+R to display a dialog box that identifies the currently selected solution and role. If you are not a member of any solution role, the **Role** field indicates that no role is selected.

Combination boxes

A combination box contains a list of items that you can select. Use the Up and Down Arrow keys to move the focus to an item. Then, press Enter to select the item.

Grids Some widgets and dialog boxes use grids that cannot be navigated by using the Tab key. For example, to navigate through the list of documents and folders in the Documents tab of the Case Information widget, use the following keys:

- Press the Tab key to move the focus into the table. The cursor moves to the column header on the first column of the table.
- Press the Tab key again to move to the table contents.
- Use the Up and Down Arrow keys to move from one row to another.
- Use the Left and Right Arrow keys to move focus from cell to cell within the same row.
- Press F2 to check a check box inside a grid cell.
- Press Ctrl+Right Arrow key to expand a twistie within the cell of a Tree Grid.
- Use Ctrl+Left Arrow key to collapse a twistie within the cell of a Tree Grid.
- Press Ctrl+F1 to display the hover help for a field on a panel after the field has focus.
- Use the Spacebar key to select a row. To select multiple rows, hold down the Shift key and press the Spacebar key. After you select a row, you can press Shift+Tab to return to the menu buttons and select the action to perform on the selected items.
- To open a selected folder or document, hold down the Shift key and press Enter.

These methods also apply to grids in the Edit Settings windows for the widgets and to the Add Members window. The Edit Settings window is used to add buttons, customize menus, or disable event broadcasting. The Add Members dialog window is used to manage roles or to add workgroup members.

Menus

Press the Alt key and then press the Spacebar key to open the **Program** menu from the left icon on the title bar of the web client. When this menu is open, pressing the Alt key closes the menu.

Solution icons

To select an icon when you create a solution, press the Tab key to move the focus from one solution icon to another. Then, press Enter to select the icon.

Navigation trees

You cannot select an item by typing characters or pressing Backspace in the navigation tree.

If you have Java™ 2 Software Development Kit 1.4 on your system, you can press a letter key to select the next item in the tree that begins with that letter.

List boxes, check boxes, and radio buttons

In a list box, press the Down Arrow and Up Arrow keys to browse for an item and press the Enter key to select an item. A list box is sometimes called a drop-down menu.

Within a list box, the following actions have no effect:

- Pressing the Ctrl key with Page Up, Page Down, Home, or End
- Pressing Shift+F8

You can select individual radio buttons by pressing the Tab key and then the Spacebar key or by using the access keys. Arrow keys do not select radio buttons within a group. Within a group of radio buttons, use the arrow keys to move the selection from one radio button to another radio button in the group. Press the Down Arrow key at the end of the group to return the focus to the first item in the group.

Additional keystrokes

Pressing Shift+Delete has no effect on text fields.

Press Ctrl+Z in a text field to undo a copy or paste action in that field.

Step Designer

The following keys are used in Step Designer:

- Ctrl+Delete to delete a highlighted object on the canvas
- Alt+Insert opens a dialog box for object insertion
- Ctrl+Space to select connectors
- Alt+Up Arrow key to select a lane
- Ctrl+Home or End key to select a step

Rule Designer

The following keys are used in Rule Designer:

- Shift+Tab to move the focus between the buttons, editor area, and error pane, and to move between completion menu options
- Left and Right Arrow keys to move the focus between the toolbar buttons and select options when you add custom rule parameters
- Spacebar to select and clear the completion menu options
- For table-based rules, use the Up, Down, Left, and Right Arrow keys to move between cells, and use Page Up and Page Down to scroll up and down the decision table

Properties View Designer

The following keys are used to move between palettes:

- Ctrl+Shift+C to move to the containers palette
- Ctrl+Shift+F to move to the properties palette
- Ctr+Shift+G to move to the settings palette for a selected element
- Ctrl+Shift+V to move to the design canvas

The following keys are used to move between the design and source tabs:

- Ctrl+Shift+D to move to the design tab
- Ctrl+Shift+M to move to the source tab

The following keys are used to move between elements on the palettes:

- Up Arrow and Down Arrow keys to move from element to element
- Alt+Down Arrow to move into nested elements
- Alt+Up Arrow to move out of the nested elements

- Home to select the first element
- End to select the last element
- Shift+Up Arrow or Down Arrow key to select a range of elements
- Shift+Home to select from the current element to the first element
- Shift+End to select from the current element to the last element
- Space to select highlighted elements
- Ctrl+Space to toggle the selection of highlighted elements
- Ctrl+Up Arrow or Down Arrow key to move focus without affecting selected elements
- Shift+Space for continuous selection of elements
- Ctrl+Shift+Up Arrow or Down Arrow key to select a secondary range of elements
- Ctrl+Shift+Home to select a secondary range of elements from the current element to the first element
- Ctrl+Shift+End to select a secondary range of elements from the current element to the last element

The following keys are used to move between the elements on the design canvas:

- Down Arrow key to move from outer layouts to inner layouts
- Alt+Up Arrow to move into the nested layout elements within the design canvas
- Alt+Down Arrow to move out of the nested layout elements
- Shift+F10 to open the context menu for the selected element
- Ctrl+U to move the selected element up or to the left
- Ctrl+Shift+U to move the selected element down or to the right
- Ctrl+Shift+B to paste before a selected element
- Ctrl+B to paste after a selected element
- Ctrl+Shift+N to insert before a selected element
- Ctrl+N to insert after a selected element
- Ctrl+K to show or hide extra padding (toggle action)

In addition to the preceding keys, the following keys are used within each container on the design canvas:

- Alt+Up Arrow to select the parent container
- Alt+Down Arrow to select the first child container
- Ctrl+Up Arrow to switch focus to the parent container without changing the current selection
- Ctrl+Down Arrow to switch focus to the first child container without changing the current selection

Features for accessible display

The web client has the following features that enhance the user interface and improve accessibility for users with low vision.

High-contrast mode

In Windows systems, the product supports the high-contrast mode option that is provided by the operating system. This feature supports a higher contrast between background and foreground colors.

Non-dependence on color
You do not need to distinguish between colors to use any function of this product.

No video only or audio only cues
IBM Case Manager does not use alerts or messages given that rely only on visual cues. In addition, IBM Case Manager does not contain any audio features.

Compatibility with assistive technologies

The web client is compatible with the JAWS screen reader application. The web client has the properties that are required for JAWS to make on-screen information available to visually impaired users.

To access pop-up dialog windows, including error messages, use the JAWS keystrokes that are designated for working in dialog boxes. For example, to access the entire content of the dialog window, press Insert+B. You can use JAWS with the Virtual PC Cursor on to read the screen and its contents, but you must turn off the Virtual PC Cursor to use the functions of the page.

Requirement: Always start the JAWS screen reader by using the **java** command instead of the **javaw** command. If you start the screen reader by using the **javaw** command, the screen reader does not work properly.

Tip: To ensure that JAWS reads the screen completely, turn off the Virtual PC Cursor.

IBM Forms application

IBM Case Manager supports more than one application for creating and using forms in your solution. For accessibility, use IBM Forms.

Product documentation

Documentation for this product is available in accessible formats.

Documentation is available in HTML format. With the HTML format, you can view documentation according to the display preferences set in your browser. It also allows the use of screen readers and other assistive technologies.

Documentation is also available in PDF format.

Designing your case management solution and application

Before you begin designing, you must prepare the design environment. Next, design your case management solution first on paper, then build it in the Case Manager Builder.

Preparing the design environment

To prepare your design environment, you can import metadata from the production environment in which you plan to deploy the solution. You can also import a solution template so that you can quickly design a new solution that is based on the template.

Related tasks:

"Preparing for solution migration" on page 117

Copying existing metadata into the case management development environment

You can use FileNet® Deployment Manager to export and import FileNet P8 assets from the object store in a production environment into the IBM Case Manager development environment target object store. You can then use those assets, mainly metadata, when you design a solution. For example, you can reuse property templates, document classes, or choice value lists from the production environment where the solution will be deployed.

About this task

Reusable assets are limited to document subclasses, property templates, non-hierarchical choice lists, or other classes, such as custom object subclasses. Additionally, because you can reinitialize the target object store, IBM Case Manager provides a method for you to store the exported metadata in a location in the design object store so that the target object store can be automatically repopulated with this metadata when the environment is reset.

Procedure

To reuse metadata from an object store when designing your solution:

1. See the FileNet Deployment Manager documentation for details on exporting and importing metadata for the steps in this procedure.

2. In FileNet Deployment Manager, create and save an export manifest of the wanted metadata from the production object store that contains the items that you want to reuse. FileNet Deployment Manager saves the new export manifest as an XML file with the name that you specified in the following directory: *deployment_location*\Environments*source_environment*\Assets\ExportManifests.
3. Create the deploy dataset. FileNet Deployment Manager uses the export manifest file to generate a deploy dataset of exported objects. The dataset directory includes a set of files where the exported metadata is stored.
4. Convert the objects in the export files for import. FileNet Deployment Manager creates the converted data set in a new subfolder of the folder that you specified. The subfolder is named after the deploy dataset name with `.converted` appended to the name.
5. Make a note of the converted data set location and directory name.
6. Import the exported metadata into the case management development environment target object store. Select the following options:

Table 1. Import options

Option	Specify
Deploy Dataset	The deploy dataset directory with the converted export objects.
Storage Policy for Imported Objects	As the exported data is metadata only, no content is present.
Import Security Permissions	Select this option to include security permission lists for the objects imported into the target object store. A permission list consists of an Access Control List (ACL) for an object. By default, this option is selected.
Import Owner	Select this option to include the owner information in the target object store. By default, this option is selected.
Import Object ID	Select this option to import the existing ID of the imported objects, allowing object relationships by ID to be maintained. If the option is not selected, the import process generates new object IDs. By default, this option is selected.
Use Original Create/Update Timestamps and Users	Select this option to preserve the source system property settings for Creator, DateCreated, DateLastModified, and LastModifier. These property values in the converted objects are carried over into the target environment. By default, this option is selected. This option requires privileged write access (AccessRight.PRIVILEGED_WRITE). See the IBM FileNet P8 documentation's security topics for more information about this permission.

Table 1. Import options (continued)

Option	Specify
Update Options	These options affect objects that already exist in the target object store. **Update if newer** The object in the destination is only updated if the object being imported has been modified more recently. **Always Update** The object in the destination will always be updated, even if it has been modified more recently than the object being imported. **Never Update** The object in the destination will never be updated, even if the object being imported has been modified more recently.

7. To simplify resetting the development environment, add the exported deploy dataset to the data set document object that is located in the reinitialization folder for the case management design object store.
   a. In IBM Administration Console for Content Platform Engine, select the case management design object store.
   b. Click **Browse** > **Root Folder** > **IBM Case Manager** > **Datasets** > **DevEnvReinitInfo** > **dev_env_connection_definition**.
   c. On the dev_env_connection_definition page in the right pane, click **DeployDataset** in the **Containment Name** column.
   d. On the DeployDataset page, click **Actions** > **Checkin, checkout, cancel** > **Exclusive checkout**, and then click **Actions** > **Checkin, checkout, cancel** > **Checkin**.
   e. In the Checkin document window, add the following exported deploy dataset XML files by clicking **Add** to navigate to the converted deploy dataset folder and attach each XML file that is contained in that folder.
      - `Catalog.xml`
      - `deployDataset1.xml`

      Restriction: Do not change the names of the `Catalog.xml` and `deployDataset1.xml` files. If you change the names, then Case Manager Builder cannot read the files.
   f. Click **Checkin**.
8. Notify the business analyst that the object store is ready for use with the imported data.

"Creating a list of object store properties and document types"

Related concepts:

Deployment overview

Creating a list of object store properties and document types

You can reuse existing Content Engine properties and document types in your case management solutions. You can create text files that provide the information from a target object store that you need for reusing existing properties and document types.

About this task

You can use the IBM Case Manager configuration tool to create two comma-separated value text files, `PropertyTemplates.csv` and `DocumentTypes.csv`.

The `PropertyTemplates.csv` file contains the following values for the properties in the object store:

- Property Template Display Name
- Symbolic Name
- Data Type
- Description
- Cardinality (single value or multi-value choice list)
- Default Value
- Min Value
- Max Value
- Max Length
- Choice List
- Required
- Hidden

The `DocumentTypes.csv` file contains the following values for the document types in the object store:

- Display Name
- Symbolic Name
- Descriptive Text
- Is Hidden
- Is Persistent
- Properties (symbolic names of properties associated with this document type)

Creating a list of object store properties and document types applies only in the development environment.

Procedure

To create a list of the object store properties and document types in an object store:

1. Start the configuration tool by running one of the following commands:

Operating system	Command
AIX®	1. Change to the *_install_path*`/configure` directory. *_install_path* is the location where IBM Case Manager is installed, for example, `/opt/IBM/CaseManagement`. 2. Run the following command: `./configmgr`

Operating system	Command
Linux	1. Change to the *_install_path*/configure directory. *_install_path* is the location where IBM Case Manager is installed, for example, /opt/IBM/CaseManagement. 2. Run the following command: ./configmgr
Linux for System z®	1. Change to the *_install_path*/configure directory. *_install_path* is the location where IBM Case Manager is installed, for example, /opt/IBM/CaseManagement. 2. Run the following command: ./configmgr
Windows	Perform one of the following actions: • Click **Start** > **All Programs** > **IBM Case Manager** > **Case Manager Configuration Tool**. • Run the following command: *_install_path*\configure\configmgr.exe *_install_path* is the location where IBM Case Manager is installed, for example, one of the following directories: – C:\Program Files\IBM\CaseManagement – C:\Program Files (x86)\IBM\CaseManagement

2. Click **Tools** > **List Property Templates and Document Types** to create the list of properties by using the wizard.
3. Provide copies of the CSV files to your business analysts who design solutions in Case Manager Builder. You can open the CSV files in a text editor, a spreadsheet, or other program to review the list of available document types or property templates and their settings.

Importing the solution template to the target environment

After you create the solution template in the source environment, you can import it to the target environment.

Before you begin

Be sure to have your completed configuration checklist available.

Procedure

To import a solution template:

1. Copy the compressed file that contains the exported solution template package to the target environment.
2. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   http://*server*:*port*/navigator/?desktop=icmadmin
   server is the IBM Content Navigator IP address or fully qualified server name.
   port is the IBM Content Navigator port number.
3. In the navigation tree in the left pane, select the object store to which you want to import the solution template and click **Solution Templates**.

4. On the Solution Templates page in the right pane, click **Import** and complete the wizard steps.

   "Creating a solution from a template"

Related tasks:

"Creating and distributing IBM Case Manager solution templates" on page 34

Creating a solution from a template

You can create a solution that is based on a solution template to quickly design a new solution. The template provides a basic design for your solution, and you can customize the new solution later in Case Manager Builder. Your administrator determines the templates that are available in an object store.

About this task

The new solution is created in the same object store as the template, and you can select the project area to which to assign the solution.

When you create a solution from a template, you can select an option to use existing unique identifiers. The default setting is the option that is set in the template.

Important: In most templates, the default behavior is to create new unique identifiers when a solution is created from the template. Do not change the option that was set in the template unless you have a specific business reason to override the default setting. If you select **Include existing unique identifiers**, you cannot deploy more than one solution that is based on this template to the same target object store.

Restriction: You cannot create a solution from a template that has files that are checked out.

Procedure

To create a solution from a template:

1. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   `http://server:port/navigator/?desktop=icmadmin`
   server is the IBM Content Navigator IP address or fully qualified server name.
   port is the IBM Content Navigator port number.
2. In the navigation tree in the left pane, select an object store and click **Solution Templates**.
3. On the Solution Templates page in the right pane, select a template.
4. Click **Actions** > **Create Solution** and complete the wizard steps.

What to do next

If the solution is associated with an IBM Business Process Manager process application, complete the steps in Copying IBM Case Manager solutions that are associated with IBM Business Process Manager process applications.

Designing your case management solution

To design a case management solution, identify what user tasks are needed to accomplish the main user goal. Decide what business level tasks and steps you need, and then group those tasks and steps into a case. As you identify the content needed to complete those steps, decide who will work on the content and what does or does not need to happen to complete it.

One approach to designing a solution is to first identify the types of documents that people in your organization need to complete for some task. For example, to resolve a credit card dispute claim, you might need a dispute form and customer to complete the form and a service representative to review that form. Next, you might need to initiate a fraud investigation if circumstances warrant such a task. In that case, you might need a fraud investigator to review the claim.

Therefore, for a credit card dispute case, the solution must include these artifacts:

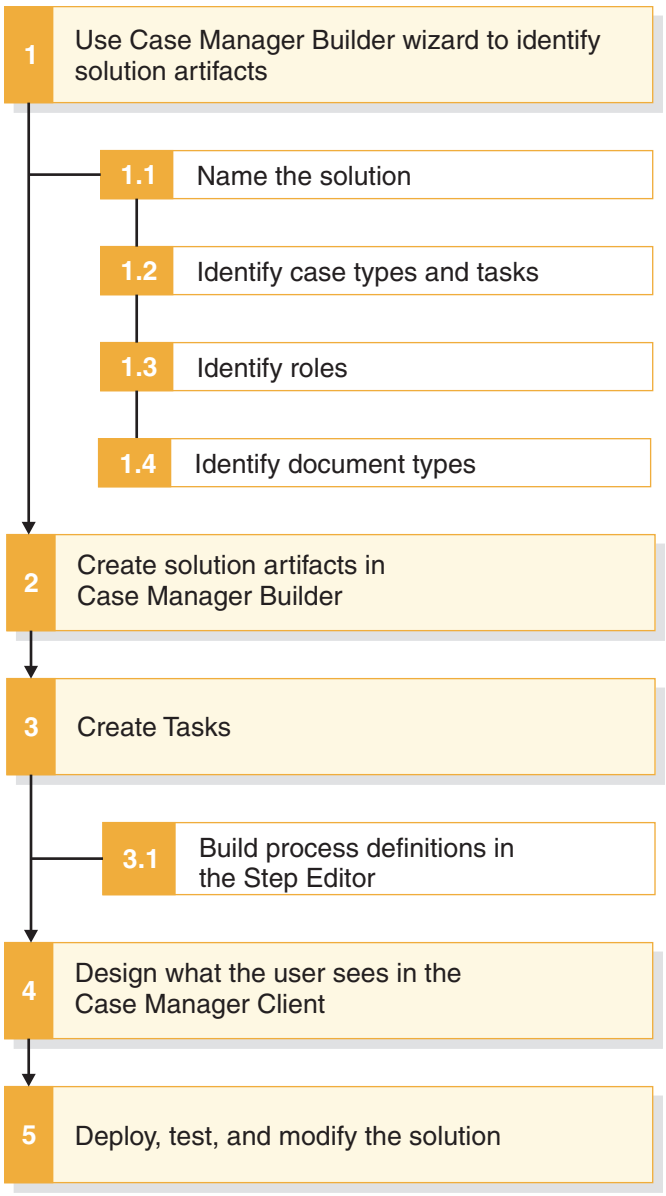
- Dispute form
- Fraud investigation form

Your solution must also include these roles:

- Customer
- Customer service representative
- Fraud investigator

The following diagram shows the steps you might take when you try to identify the artifacts that you will need for a solution.

You can use Case Manager Builder to help you think through the various document types, roles, case types, tasks, and so on that you need for a specific solution.



A solution is a set of related business problems (or case types). For example, if you are designing a solution for the bank industry for a credit card dispute claim, you might first decide what case types are needed. An example of a credit card dispute case type is a processing a claim. For this case type, a customer claim for a credit card dispute is reported and processed.

For every business problem that you are trying to solve (case type), you have physical assets or documents (document types) that you work with to complete the case, people who work those documents (roles), and tasks that need to be completed to close the case. Properties help to define the details of the case types, document types, roles, and tasks.

A process describes how case workers must complete a task, but a task describes what needs to be done and why. For every task, steps can be completed by the system or by the case worker. Tasks can be run in parallel, they can be chained together, or they can even be skipped.

You can define a task process map by using Step Designer in Case Manager Builder or by using Process Designer, which is integrated into Case Manager Builder at both the solution and task level. You can create a Case Manager Builder process definition by using the Step Designer or an external process from IBM Case Foundation or IBM Business Process Manager. You can modify workflow processes that are created for a task in the Case Manager Builder Step Designer in the FileNet P8 Process Designer. External process tasks are created as reused tasks in the Case Manager Builder and should be implemented by using FileNet P8 Process Designer or Integration Designer.

Tasks can be required or optional, and you can set the tasks to start automatically or manually by a case worker. A case is completed when all required and currently running tasks are completed. In addition, you can group tasks so that they are mutually exclusive and only one task in the group can be completed or all-inclusive and all tasks in that group must be completed. You can also group tasks inside of a container task.

You can also associate business rules with your solution. Organizations might have rules for business operations, such as for pricing calculations, eligibility checks, validations, underwriting, and fraud detection. In your solution, you can create business rules that determine process routing or update case properties. In conjunction with other IBM Case Manager capabilities, business rules can be used in the following ways:

- Intelligently assign priority to cases or assign case workers to tasks
- Automatically create and assign tasks
- Trigger fully automated actions that are based on external events, completion of other case tasks, or expiration of task deadlines
- Apply rules to the key facts and information, and guide the responses that are based on that information
- Simplify certain tasks by automating the decision logic
- Increase consistency by using decision rules across similar cases

You can also design your solution in other ways:

- Decide what the case worker needs to do to complete his or her job and what fields are needed in the Case Manager Client.
- Evaluate the use case flow and extract the solution assets from it.

As you become familiar with designing solutions, you can identify the roles, document types, and properties that can be used in more than one case type.

Tip: When multiple business analysts are collaboratively designing a solution, inform other users before you delete solution objects such as case types. If you delete a case type and commit the changes while another user is editing that case type, errors will be returned when that user saves and deploys the solution.

When you design and create a solution, you must decide what the solution locale is. The solution locale refers to the locale of display names, such as case properties, case types, tasks, and other solution artifacts that you create with Case Manager Builder. When you deploy the solution to a target environment for the first time, you must deploy the solution under the same locale to ensure that the display names are preserved.

"Identifying your solution artifacts" on page 16

"Creating a solution description document" on page 17

Related concepts:

- Case management overview
- Case management solution concepts
- Case Manager Builder
- Case Manager Client

Identifying your solution artifacts

When you design your solution, identify the document types that are needed for the cases. Then, decide which people must be involved and what they will work on.

In the credit card dispute solution, the document types that you might need are a dispute form, a transaction statement, or a correspondence letter. The people who will work on these document types might be the customer, a customer service representative, a dispute advisor, the merchant, or a chargeback advisor.

Next, decide what sort of tasks will be needed and why. For the credit card dispute, you might have the following tasks:

- Receiving a form from a customer
- Initiating the case
- Tracking the case status
- Reviewing a document
- Requesting a copy of the sales
- Opening a dispute claim
- Opening a fraud investigation
- Generating correspondence
- Requesting a document

For each task, you must decide who will be working on the task, when does the task need to be worked on in the case life cycle, and how the task needs to be implemented.

For the task that initiates the process, you must create roles for the customer and the customer service representative. This task likely needs to be the first task in the case life cycle. This task also could be an automatic task that has no preconditions. As an automatic task with no preconditions, the task will start when the case is started and can even be chained to subsequent tasks.

Create steps to map how the task is implemented. The steps for that task might be answering a customer phone call, gathering customer information, retrieving customer data, or providing supporting documentation. You can define rule steps to automatically determine process routing or update a case according to a business rule. For example, you can add a rule step to determine the customer rating, such as DIAMOND, GOLD, or SILVER, that is based on the total transaction amount and how long the person has been a customer.

A precondition for the task to start could be that the case was opened by the customer service representative in the Case Manager Client when receiving the customer call.

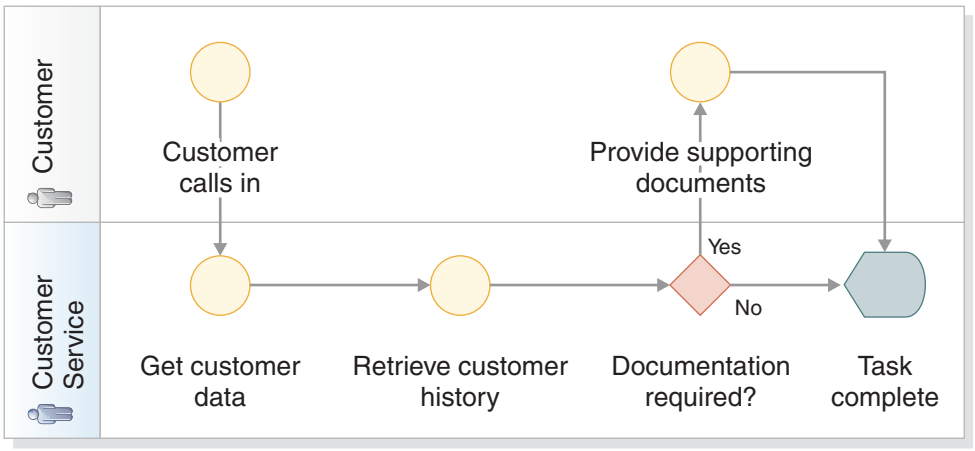


Figure 1. Flow diagram of the task: Initiating Case

After you identify the document types, roles, and tasks, decide which properties will make up the solution. The properties for the credit card dispute cases might be card reason code, customer ID, dispute priority, or exposure amount.

After you identify the properties of your solution, specify your decisions about document types, case types, steps, preconditions, and so on in Case Manager Builder.

Related concepts:

- Case management overview
- Case management solution concepts
- Case Manager Builder
- Case Manager Client

Creating a solution description document

You can generate a solution description document by running the Solution Document Generator from a command line. The solution description document includes a list of the assets that are defined in Case Manager Builder.

About this task

A solution consists of a set of cases and supporting information, including a definition file that describes the overall structure and contents of the solution, a set of XPDL files describing workflows that are associated with the cases in the solution, and a Process Engine configuration file that contains the Process Engine configuration details, such as queue, role, in-basket, roster, event log, application space, and step processor definitions for the solution.

The Solution Documentation Generator creates a solution description document that provides a summary of the contents of the solution definition file (SDF), XPDL files, and the Process Engine configuration file. The solution description document does not list rules, views, and pages.

When you design solutions, you can use the solution description document to view the organization of the solution and its contents in an easy-to-read format that can be shared with case workers and customers.

You can create a solution description document for only one solution at a time. You can choose from one of the following types of output: PDF, Microsoft Word, or XHTML.

Procedure

To generate a solution description document:

1. Navigate to the Solution Documentation Generator location:

Operating system	Location
AIX	`/opt/IBM/CaseManagement/docGenerator`
Linux	`/opt/IBM/CaseManagement/docGenerator`
Linux for System z	`/opt/IBM/CaseManagement/docGenerator`
Windows	`C:/Program Files/IBM/CaseManagement/docGenerator/`

   Restriction: For the Solution Documentation Generator to successfully create solution description documents, the IBM Case Manager installation path cannot contain special non-English characters or symbols.

2. Open the `docGenerator.properties` file in a text editor and define your IBM Case Manager environment.
   a. For the `ceURI` property, enter the full URI of the Content Engine server. For example, http://*localhost*:9080/wsi/FNCEWS40TOM.
   b. For the `objectStoreName` property, enter the name of the design object store that contains the solution that you want to generate a solution description document for.
   c. For the `solutionName` property, enter the name of the solution that you want to generate a description document for.
   d. For the `outputFormat` property, enter the output format for the solution description document.

      PDF To get an Adobe Acrobat PDF file.

      Word To get a Microsoft Word Rich Text Format (RTF) document.

      HTML
      To get an XHTML file.
   e. For the `outputLocation` property, enter the directory location where you want the solution description document to be created.
   f. Optional: For the `antOpts` property, enter the maximum memory to be allocated to the JVM for a large solution.

   The following example shows an example of a `docGenerator.properties` file:

```
ceURI = http://myServer:9080/wsi/FNCEWS40MTOM
objectStoreName = CMDOS
solutionName = MySolution
outputFormat = PDF
outputLocation = C:/IBM/CaseManagement/docGenerator/output
antOpts = -Xmx2000m -Dmax JavaMemory=2000m
```

   Tip: For the **`outputLocation`**, you must use a forward slash (/) to separate folder names in the properties file regardless of your operating system type.

3. Open a command prompt and run the Solution Document Generator. You can append a parameter to the command to check in the generated document into the FileNet repository: **checkin**.

   The **checkin** parameter checks in the solution description document into the same object store in the solution folder. By checking in the solution description document into the same folder as the solution, you can iteratively monitor how the solution design changes.

Operating system	Command
AIX	`docgen.sh`
Linux	`docgen.sh`
Linux for System z	`docgen.sh`
Windows	`docgen.bat`

   For example, enter `docgen.bat -checkin`

4. At the prompt, enter a user name and password that can retrieve and add content to Content Platform Engine.

Results

The Solution Document Generator produces a document with the name of the solution and an extension that is appropriate for the output format. The document is added to the location that is specified in the properties file, for example: `C:/IBM/CaseManagement/docGenerator/Output/MySolution.pdf`. The document is also checked into the design object store in the solution folder if you provide a **checkin** parameter.

Sample business rules

Business rules can include user-defined case properties and case system properties. Business rules can also include custom rule parameters if you want the rule to refer to data that is external to the case.

Including various types of case properties in a rule

The following sample business rule sets the customer ranking for the account holder to Gold if the current account balance is more than 1 million dollars, the credit rating of the account holder is more than 75, and at least one of the following conditions are true:

- A salary is directly deposited into the account each month
- The account was open for more than three years

If the conditions are not met, the associated rule step returns the specified print statement to the workflow so that the value can be used by the next step in the workflow.

The rule includes a temporary variable, customerAccountBalanceAsOfToday, that is set to the value of the current account balance.

The rule includes the following properties from the BankAccountUpdate case type:

Name	Type
AccountBalance	Float

Name	Type
isSalaryAccount	Boolean
RelationshipStartDate	Datetime
CustomerCategory	String that is associated with a choice list that has the values GOLD, SILVER, and NORMAL

The rule also includes the following custom rule parameters that are defined in the Case Manager Builder rule designer and are mapped to external data sources in Process Designer. For more information about mapping custom rule parameters to external data sources, see Mapping custom parameters in rule steps to external data sources.

Name	Type
CreditRatingFromExternalAgency	Integer
RelationshipDurationInMonths	Integer. The value of this parameter is derived by using a Process Designer expression that uses the RelationshipStartDate case property and the system time.

```
definitions
  set 'customerAccountBalanceAsOfToday' to the AccountBalance of BankAccountUpdate ;

if all of the following conditions are true :
- customerAccountBalanceAsOfToday is more than 1000000
- CreditRatingFromExternalAgency is more than 75
- any of the following conditions is true :
   - BankAccountUpdate is isSalaryAccount
   - RelationshipDurationInMonths is more than 36

then set the CustomerCategory of BankAccountUpdate to GOLD ;

else print "No changes were made to the customer category by the rule: "
+ the name of this rule ;
```

Determining process routing

The following sample business rule is used to determine process routing. Based on whether the account holder is included in a list of defaulters that is obtained from an external data source, the rule returns a print statement to the workflow to indicate whether to accept the overdraft request. The specified print statement can be used by the next step in the workflow, such as to display the print output on the Case Details page to advise the case worker how to proceed. Alternatively, you can create a step in Process Designer to automatically trigger a response that depends on the value of the print output.

The rule includes the following property from the BankAccountUpdate case type:

Name	Type
AccountHolderName	String

The rule also includes the following custom rule parameter that is defined in the Case Manager Builder rule designer and is mapped to an external data source in Process Designer:

Name	Type
ListOfDefaulters	String, multiple value

```
if the AccountHolderName of BankAccountUpdate is one of ListOfDefaulters
then print "REJECT THE OVERDRAFT REQUEST PENDING SUPERVISOR APPROVAL";
else print "SEND THE REQUEST FOR SENIOR MANAGER REVIEW";
```

Related concepts:

Business rules

Related tasks:

"Adding rule operations to a task by using Process Designer" on page 23

IBM Case Manager tour: Create business rules

Related information:

"Troubleshooting overlap and gap warnings in table-based rules" on page 219

Configuring auditing

You can configure auditing for use with the analytics tools that are supported by Case Analyzer. You can also configure auditing to track the history of cases by using the Timeline Visualizer widget. You can configure auditing for a deployed solution in a development environment, or in a production environment.

About this task

Choose properties to audit that are meaningful to your business and solution. For example, a financial organization might want to audit properties such as LoanAmount, ApprovalStatus, and Priority. A case analyst might be interested in the number of occurrences of a particular case type, or the length of time that case workers require to complete a particular task.

You specify properties to audit by using the audit configuration wizard in the IBM Case Manager administration client. Select document properties and properties of each case type for the solution that you want to audit. If there are tasks defined for the case type, you can select the task and then select the task properties that you want to audit. To view custom properties in the extended history, you must select those properties for auditing. In addition, some system properties are automatically selected for auditing.

Tip: To save disk space, improve performance, and avoid displaying unnecessary data, do not audit properties with values that are unlikely to change. You can obtain the values of these properties from the case objects.

Audit configuration settings are stored in an audit manifest file. You can move an audit manifest from one environment to another by using the export and import audit configuration wizards. For example, you can create and check your audit configuration in a test environment before you import the audit configuration into production.

After you specify properties to audit and apply the audit configuration to a solution, you can use Case Analyzer to generate chart-based reports that are based on statistical information that is gathered from the system. For information about additional configuration steps that are required before you can use Case Analyzer and other case analytics tools, see Integrating IBM case analytics tools.

To track the extended history of cases by using the Timeline Visualizer widget, you must define a case history store. You can store extended case history data in the database instance that is used for the target object store. Alternatively, you can store extended history data in a separate database instance. For example, you might want to use a separate, remote database server if the I/O throughput is problematic. For more information, see "Preparing a database for the case history store" on page 61.

Procedure

To configure auditing:

1. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   `http://server:port/navigator/?desktop=icmadmin`
   server is the IBM Content Navigator IP address or fully qualified server name.
   port is the IBM Content Navigator port number.
2. In the navigation tree in the left pane, select a design object store and click **Solutions**.
3. On the Solutions page in the right pane, select the solution that contains the properties you want to audit.
4. Click **Actions** > **Manage** > **Audit Configuration** and complete the wizard steps. You can create an audit configuration, or edit an existing audit configuration. You can save your changes, however, the audit configuration will not take effect until you apply it.
5. If you plan to use the Timeline Visualizer widget, you must prepare a database to record extended case history data. Then, configure and enable the case history store.

   Attention: If the Content Platform Engine server that serves as the backend to the IBM Case Manager system is configured as a cluster, configure and enable the case history store when only a single Content Platform Engine server is available. This is typically during a maintenance window when all but one of the application server instances hosting the Content Platform Engine server can be stopped.

   To configure and enable the case history store:

   a. In the IBM Case Manager administration client, in the navigation tree in the left pane, select a target object store and click **New Case History Store**.
   b. Complete the wizard steps.

Related concepts:

Timeline Visualizer widget

Related tasks:

"Preparing a database for the case history store" on page 61

"Exporting the audit configuration" on page 134

"Importing the audit configuration" on page 155

Integrating with IBM FileNet Case Analyzer

Related information:

Product Documentation for IBM FileNet Case Analyzer

Adding rule operations to a task by using Process Designer

You can use rule operations to run business rules in a workflow. For example, you can use rule operations to determine process routing or update case properties.

Before you begin

In Case Manager Builder, define the business rule that you want to run.

In Process Designer, define a data field of type string to store the return value that is the output of the rule operation.

You must also define a data field for each custom rule parameter that is associated with the rule that you want to run. If your rule includes a custom rule parameter in a condition, you must define a data field whose value is populated by a previous step in the workflow. If your rule includes an action that sets the value of a custom rule parameter, you must define a data field whose value is set by a later step in the workflow.

About this task

To add rule operations, you open the task in Process Designer and add a component step to the workflow with which you associate the rule operation. The return value of the rule operation is a string that contains a concatenation of all the print statements that are outputs of the rule.

All case properties that are updated by the rule are updated in Content Platform Engine.

Procedure

To add rule operations to a workflow step:

1. In Case Manager Builder, click the **Open Process Designer** icon for the task to which you want to add the rule operation.
2. In Process Designer, drag the **Component** icon to the location in the task flow where you want the operation to be run.
3. On the **Component** tab, click the **Add** icon.
4. From the **Component** list, select **ICM_RuleOperations**.
5. Select the **executeRule** operation.
6. In the **Operation Parameters** area, enter an expression for each operation parameter by clicking in the **Expression** field and selecting **Build Expression**.
   a. For the **caseID** parameter, select **F_CaseFolder** from the **Business Object Fields** list.
   b. For the **ruleName** parameter, specify the unique identifier of the rule that you want to run. For example, specify `"myRule"`.
   c. For the **customRuleParameterNames** parameter, enter a string expression that lists the unique identifiers of all custom rule parameters that are associated with the rule. For example, specify the expression `{"Param1","Param2","Param3"}`.
   d. For the **customRuleParameterValues** parameter, enter a string expression that specifies the data fields to map to the custom rule parameters that are associated with the rule. Ensure that you specify a value for each custom rule parameter and that you list the values in the same order as the custom

rule parameter names are listed in the **CustomRuleParameterNames** parameter. For example, specify the expression {dataField1,dataField2,dataField3}.

For data types other than string, you must create an expression that gives the value of the data field in a textual form. For example, to convert the Created Date property of the case to a string, use the following pattern: timetostring(F_CaseFolder.DateCreated,"yyyy-mm-dd hh:tt:ss")

For multiple-value custom rule parameters, specify the value in the format arraytoString(*data_field*,"{","}",","). For example, if your rule uses the InterestRate and CreditRatings custom rule parameters, and you defined data fields with the same names, specify the following value for the **CustomRuleParameterValues** parameter:

{InterestRate,arraytoString(*CreditRatings*,"{","}",",")}.

e. For the **return_value** parameter, specify the name of the data field to store the return value that is the output of the rule operation. For example, specify "dataField4".

Related concepts:

"Cannot access Process Designer from Case Manager Builder with Google Chrome" on page 230

Business rules

Related reference:

"Sample business rules" on page 19

Configuring the in-basket property synchronization settings

When a property value is updated in a case, the change is synchronized in all views of the case. You might experience performance issues if all property updates are set to synchronize automatically. To improve performance, you can disable the automatic synchronization for certain properties.

About this task

When you tune the property synchronization settings for performance reasons, choose properties that are not frequently updated.

At design time, you use Process Designer to save the event update settings as part of the solution. For solutions that are already deployed, you use Process Configuration Console to change the settings.

Procedure

To configure property synchronization settings:

1. From the Manage Solutions page in Case Manager Builder, click the Process Designer icon on the solution that you want to configure.
2. Click **View Configuration**.
3. In the left pane, expand **Work Queues**, right click the queue that you want to configure, and select **Queue Properties**.
4. On the Data Fields tab, clear the checkbox in the Event Update column for all properties that you want to disable synchronization for.
5. Commit your changes.

Related concepts:

"Cannot access Process Designer from Case Manager Builder with Google Chrome" on page 230

Validating preconditions

Run the precondition checker utility to validate preconditions after changing property preconditions for an existing task. The precondition checker looks for tasks that were created before the precondition changed and evaluates the updated task. If the new precondition is met, the task status changes to working status.

preconditionChecker

The precondition checker utility updates solution tasks in which the following changes were made:

- The criteria changes for a task with a **A property condition is met** precondition.
- The precondition changes from **A document is filed in the case** or **A case property is updated** to **A property condition is met**.
- Or, any precondition changes to **No precondition**.

Tip: You do not need to deploy the solution after you run the precondition checker utility.

The precondition checker utility is in the IBM Case Manager installation folder.

Table 2. Precondition checker file name and location

Platform	File name	Location
AIX	`preconditionChecker.sh`	`/opt/IBM/CaseManagement`
Linux	`preconditionChecker.sh`	`/opt/IBM/CaseManagement`
Linux for System z	`preconditionChecker.sh`	`/opt/IBM/CaseManagement`
Windows	`preconditionChecker.bat`	`C:\Program Files\IBM\CaseManagement` for a fresh install `C:\Program Files (x86)\IBM\CaseManagement` for an upgrade

Syntax

preconditionChecker *command parameter value*

Commands

`launch`
Start the precondition checker utility. The **launch** command requires parameters.

`suspend`
Stop the precondition checker utility. The **suspend** command does not require parameters.

Parameters

`-cews_uri`
The web services URI to connect to Content Engine. For example http://myserver:9080/wsi/FNCEWS40MTOM. Required.

`-username`
The user ID to connect to Content Engine. Required

-password
The password for the specified user ID to connect to Content Engine. If not specified, the precondition checker utility will prompt for the password. Required.

-target_os
The target object store that the precondition checker will check. Required

-solution
The name of the solution that the precondition checker will check. Optional. If no solution is specified, the precondition checker utility checks all deployed solutions.

If the name of the solution includes spaces, surround the name with single quotation marks. For example, `-solution 'my long solution name'`.

-file
The path to an input file that contains the precondition checker parameters. Optional.

If specified, the input file must include the **cews_uri**, **username**, **password**, and **target_os** parameters, without leading dashes.

-batchSize
The number of items to retrieve and process at one time. If not specified, the default batch size is 1000 items.

-threadPoolSize
The number of active threads when processing tasks. Optional. The default value is four threads.

```
preconditionChecker launch -cews_uri http://myserver:9080/wsi/FNCEWS40MTOM
-username administrator -password mypassword
-target_os MyTargetOS -solution 'credit card dispute'
```

Resetting the test environment

You can use the Case Manager Builder **Reset Test Environment** feature to remove the deployed solutions and other data from the development environment project area.

Before you begin

Ask your system administrator to temporarily increase the timeout values for the WebSphere Application Server transaction service, ORB service, and target object store data source connection pools for both the IBM Case Manager and Content Platform Engine application servers. The optimal timeout values depend on the speed and complexity of the system. For example, 1200 seconds is appropriate for most systems. In addition, reset the initial and maximum heap size for the same application servers as needed, according to the number of applications that are running on the servers. For example, set the initial heap size to 512 MB and set the maximum heap size to 1024 MB or a size that is consistent with the available RAM on the server.

After the reset actions complete, the system administrator can reset the timeout values and heap sizes to the previous values.

About this task

Over time, you might need to reset the development environment to provide a clean environment for further development and testing. Resetting the test

environment returns the project area in the case management object store to the same state as just after you completed the configuration tasks. The target object store and the connection point that is associated with the project area are reinitialized, and all process configuration information is removed.

Because you might have several people working in the development environment on multiple projects, you can define project areas to limit the effects of resetting the test environment. For example, you can group users that are working on related solutions in the same project area. Therefore, when you reset the test environment, only the solutions and artifacts in one project area are removed. The entire design object store is not affected, and other Case Manager Builder users can continue working without interruption.

Important: Resetting the test environment removes all of the data from the project area in the development environment, including any FileNet P8 assets that you copied from your production environment and any assets you defined outside of Case Manager Builder to extend the solution design, such as reused class definitions or property templates. If your environment reuses existing FileNet P8 assets to provision the development environment, certain assets can be automatically restored by the reset test environment operation if the development environment was prepared as described.

You might need to reset the environment in the following situations where modifications can only be applied to a fresh development target object store:

- Some changes are not allowed as part of solution redeployment.
- Artifacts from deployed solutions cannot be deleted by using Case Manager Builder. For example, any documents that were defined in the object store must be removed by using other tools.
- The development environment target object store might exceed the underlying database table limitations.

Tip: If your solutions are already deployed to a production object store, review the redeployment restrictions before you modify and redeploy a solution.

Procedure

To reset the test environment:

1. Ensure that other applications, such as Case Manager Client or Administration Console for Content Platform Engine, are not making changes to the target object store or querying the project area.

   Attention: Skipping this step can cause the reset operation to fail.
2. Save user-defined assets from the target object store. You might have to ask a system administrator to save the assets.
3. In Case Manager Builder, click **Actions** > **Reset Test Environment** on the Manage Solutions page.
4. If you are using Case Analyzer, use the **Reset database** option of the Case Analyzer Process Task Manager to initialize the Case Analyzer database.

"Saving user-defined assets before you reset the test environment" on page 28

Related reference:

"Redeployment restrictions for modifying a solution" on page 161

Related information:

IBM WebSphere Application Server V7.0 documentation

- IBM WebSphere Application Server V8.0 documentation
- Resetting the Case Analyzer store

Saving user-defined assets before you reset the test environment

You can use IBM FileNet Deployment Manager to save assets from the target object store before you reset the IBM Case Manager development environment project area.

About this task

When you click **Reset Test Environment** in Case Manager Builder the target object store and its associated connection point are reinitialized, and all user-defined assets are deleted. The project area target object store is restored to the state after any add-ons were configured. You can save existing assets in the design object store and automatically restore the assets to the target object store after you reset the test environment. For example, document folders, property templates, and custom object subclasses can be saved and restored.

Important: Save the user-defined assets before you reset the test environment or your user-defined assets will be deleted and cannot be restored. User-defined assets that are objects in the document class and include content must be exported by using FileNet Deployment Manager and saved externally to disk. These assets must be manually reimported into the target object store for the project area by using FileNet Deployment Manager after the reset test environment operation completes. Workflow system configuration assets that are not created in IBM Case Manager, such as component queues, must be exported and imported by using the Process Configuration Console that is accessible from the Content Platform Engine administration client.

Procedure

To save user-defined assets before you reset the test environment:

1. Create and save an export manifest of the assets that you want to save from your target object store in the test environment:
   a. Start FileNet Deployment Manager.
   b. Click **Environments** > ***environment definition*** for the environment definition that you want to export assets from.
   c. Right-click **Export Manifests** and click **New** > **Export manifest**.
   d. Open the manifest, click the **Add Assets to the export manifest editor** icon, and select the assets that you want to save from the target object store.
   e. Specify the export manifest file name, the output folder, and the deploy dataset name.
   f. Click **OK**. The export starts.
2. Add the exported deploy dataset to the `DeployDataset` set document object in the reinitialization folder for the case management design object store:
   a. In IBM Administration Console for Content Platform Engine, select the case management design object store.
   b. Click **Browse** > **Root Folder** > **IBM Case Manager** > **Datasets** > **DevEnvReinitInfo** > **dev_env_connection_definition**.

c. On the dev_env_connection_definition page, click **DeployDataset** in the **Containment Name** column.
d. On the DeployDataset page, click **Actions** > **Checkin, checkout, cancel** > **Exclusive checkout**, and then click **Actions** > **Checkin, checkout, cancel** > **Checkin**.
e. In the Checkin document window, add the exported deploy dataset XML files. Click **Add** to navigate to the deploy dataset folder that you selected when you exported the manifest in FileNet Deployment Manager, such as `...\IBM\FileNet\ContentEngine\tools\deploy\P8DeploymentData\Environments\environment name folder \Assets\`*`export manifest name folder`*, and attach the following XML files:
   - `Catalog.xml`
   - `deployDataset1.xml`

   Restriction: Do not change the names of the `Catalog.xml` and `deployDataset1.xml` files. If you change the names, then Case Manager Builder cannot read the files.
f. Click **Checkin**.

What to do next

Notify the business analyst that the object store is ready for use with the imported data.

Related information:

Create deploy dataset

WebSphere Application Server: Timeout properties summary

Copying an existing solution

You can copy an existing solution, which is assigned to the same project area in development, to quickly design a new solution that is based on the existing solution.

About this task

The copy solution operation is available in the IBM Case Manager administration client, which can be used in any domain. Project areas are only present in the development domain.

You can either reuse the existing properties or document types from the original solution, or you can select the option to create properties or document types when you deploy the new solution. When you reuse existing properties or document types in a solution, you cannot redefine them in Case Manager Builder. You can remove the property or document type from the solution in Case Manager Builder, but you cannot change any of the attributes, such as data type.

Copying an existing solution applies only in the development environment.

Restrictions:

- You cannot copy a solution that has currently running tasks or that has files that are checked out.
- You cannot copy an solution that was not yet committed.

- If a property that was not defined in the solution, such as a system property, is used as a parameter for a rule operation in a workflow, the copy solution operation will fail validation. To copy the solution, you must clear the validation checkbox.

Procedure

To copy a solution:

1. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   `http://`*`server`*`:`*`port`*`/navigator/?desktop=icmadmin`
   `server` is the IBM Content Navigator IP address or fully qualified server name.
   `port` is the IBM Content Navigator port number.
2. In the navigation tree in the left pane, select an object store and click **Solutions**.
3. On the Solutions page in the right pane, select the solution that you want to copy.
4. Click **Actions** > **Copy** and complete the wizard steps.

   "Copying a solution to another development environment"

Copying a solution to another development environment

You might need to copy a solution to another development domain for additional development and testing. After you copy the solution to the additional environment, you can open it in Case Manager Builder to edit, deploy, and test the solution in that environment.

About this task

The following diagram depicts a high-level view of the process of copying a solution to another development environment:

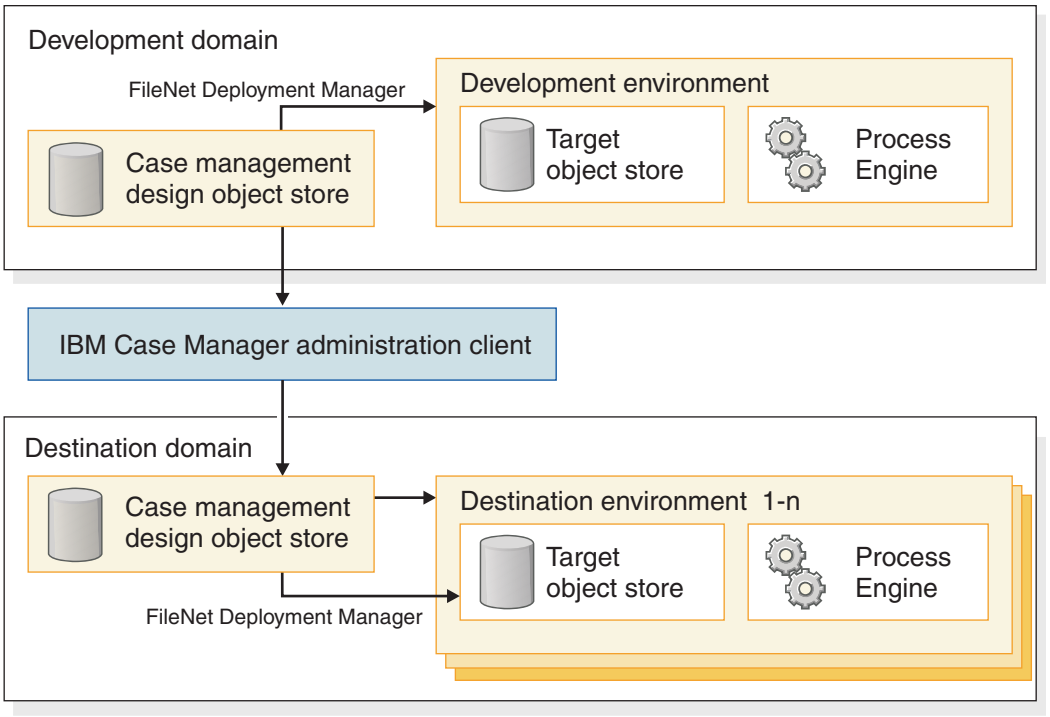


Figure 2. Copying a solution overview diagram

Procedure

To copy a solution package to a different development design object store:

1. If your solution contains assets that were created outside of IBM Case Manager, in FileNet Deployment Manager, create a deploy package that contains the assets. Then, use Administration Console for Content Platform Engine to add the deploy package to the source server design object store in the solution folder. If your solution contains marking sets, you must manually recreate the marking sets and the properties that use the marking sets in the target environment.
2. In the IBM Case Manager administration client, export the case management solution package from the source development environment case management design object store to the server where you run the IBM Case Manager administration client.
3. In the IBM Case Manager administration client, import the solution package from the local server where you run the IBM Case Manager administration client to the target environment design object store.
4. In the IBM Case Manager administration client or Case Manager Builder, deploy the solution package in the target environment.
5. If your solution contains assets that were created outside of IBM Case Manager, download the assets from the target environment design object store (from Step 3), and then in FileNet Deployment Manager, expand the assets in the target environment and then import the assets to the target object store.

   See the FileNet Deployment Manager documentation for details on the steps in this procedure: **Deploying IBM FileNet P8 applications** > **Prepare data for deployment** > **How to...** > **Prepare Content Engine data** > **Manage deploy packages**

What to do next

If your solution uses properties that are associated with marking sets, and you move the solution to a different environment, you must recreate the marking sets and any property templates that use the marking sets in the target environment. To recreate the marking sets, use the appropriate FileNet P8 tools. When you recreate the properties, you must use the same symbolic name that is used in the source environment.

If your solution is associated with an IBM Business Process Manager process application, and you copy or move the solution to a different environment, you must also copy or move the process application.

Related tasks:

Copying IBM Case Manager solutions that are associated with IBM Business Process Manager process applications

Comparing solutions

You can use Case Manager Builder to compare two solutions.

About this task

Upgrading a customized case management solution: To address the unique requirements of their organizations, customers might choose to customize the case management solutions that they use. When these customers upgrade their case management solutions, they do not want to lose any changes that they previously made to the solutions. Using the results of the solution comparison report, customers can update their customized case management solutions after they upgrade.

Merging two different solutions into a single solution: Before an IT group merges two solutions, they can use the results of the solution comparison report to determine whether conflicts exist. For example, duplicate property names represent a conflict.

Procedure

To compare solutions:

1. Log in to Case Manager Builder.
2. Find one of the solutions that you want to compare and click **More Actions** > **Compare**.

   Important: The solutions that you want to compare must be committed.

   Tip: If you plan to compare two versions of the same solution, select the older version first.
3. Select the other solution that you want to compare and click **OK**.

   Ignore solution prefixes

   Solution prefixes are unique; no two solutions have the same prefix.

   - Leave this option selected to hide the prefixes of the solutions being compared.
   - Clear this option to see the prefixes of the solutions being compared.

Ignore GUIDs of the objects

Object GUIDs are unique; no two objects have the same GUID.

- Leave this option selected to hide the GUIDs of the objects being compared.
- Clear this option to see the GUIDs of the objects being compared.

4. View the results of the comparison in the messages area of the Manage Solutions page.

High-level information

High-level information is provided for the following items:

- Pages
- Rules
- Task workflows
- Views

Detailed information

More detailed information (such as actual values) is provided for the following items:

- Case properties
- Case types
- Choice lists
- Content Platform Engine configuration values
- Document types
- In-baskets
- Roles
- Task properties
- Tasks

In the results, the solution for which you selected the **Compare** action is referred to as Solution 1, and the solution that you are comparing it to is referred to as Solution 2. The results include information about what items are different between solutions:

Modified

The item exists in both solutions, but its value is different in each solution.

Missing

The item is missing in Solution 1 (that is, the item exists only in Solution 2).

Found The item exists only in Solution 1 (that is, the item is missing in Solution 2).

Tip: The messages area is dynamic and always displays the most recent message. To give yourself time to thoroughly review the results of the comparison, copy the results to a text file. If the comparison results in the message area are overwritten before you can review them on-screen, run the comparison again.

Restriction: The solution comparison detects changes that were made to objects that are visible in Case Manager Builder only. It doesn't detect changes made by Process Designer to Content Platform Engine objects such as event logs, queues, and rosters.

"Scenario: Upgrading a customized case management solution" on page 34

Scenario: Upgrading a customized case management solution

If your organization uses a customized case management solution, you need to have an upgrade plan, which ensures that your customizations aren't overwritten from one release of the case management solution to the next. This scenario shows you one way to upgrade a case management solution, compare the new and the customized solutions to identify differences, and then use the resulting report to update your customized solution.

An IBM business partner, PartnerA, builds a case management solution for the insurance industry. PartnerA names the solution InsuranceSolution and bases the solution on a standard case solution that IBM provides. After InsuranceSolution gets great reviews from industry analysts, PartnerA sells its solution to a number of customers, including a large insurance company, CompanyB.

While using InsuranceSolution, CompanyB realizes that it needs to customize the solution to meet the specific requirements of its organization. In particular, CompanyB wants to add a property, a role, and a task, and it wants to add a choice to an existing choice list.

PartnerA advises CompanyB to make the additions to a copy of InsuranceSolution, not to customize the original solution itself. So CompanyB makes a copy of the solution, gives the copy a different name (InsuranceSolution_CompanyB) and prefix, makes the desired additions to the copy, and then deploys the copy.

When PartnerA releases a new version of its case management solution, CompanyB imports it. The new version (InsuranceSolution2) overwrites the previous version (InsuranceSolution). As a safeguard, CompanyB makes a copy of its own customized solution (InsuranceSolution_CompanyB) and archives it. CompanyB then compares InsuranceSolution2 with InsuranceSolution_CompanyB, updates InsuranceSolution_CompanyB based on the reported differences, and deploys the newly revised copy.

Creating and distributing IBM Case Manager solution templates

In addition to creating solutions for deployment in the same domain that is hosting your Case Manager Builder instance, you can create solution templates that can be distributed to a separate IBM Case Manager domain or at another site. After you design and create a case management solution, you can create a template from that solution to use as a base for other solutions.

About this task

At a minimum, a solution template must contain a solution definition file, which you create using Case Manager Builder. You create the template in the IBM Case Manager development domain, or source environment, and then distribute it to be used at a different IBM Case Manager development domain, or target environment. You do not modify a solution template directly, you modify the solution that you create from a solution template. You use the IBM Case Manager administration client to move the case management solution template between environments.

You can also distribute other types of assets:

- Other FileNet P8 assets, which are associated with the solution but managed by other FileNet P8 tools. These assets must be migrated and deployed through FileNet Deployment Manager and Process Configuration Console.

- Other IBM and external assets, which are developed outside of IBM Case Manager and FileNet P8. Manual changes are required to migrate and deploy these types of assets.

  "Converting a solution to a template"

  "Distributing solutions as templates"

Related tasks:

"Importing the solution template to the target environment" on page 11

Related information:

Copy and edit solutions with the Solution Assistant tool

Converting a solution to a template

You can convert a solution to a template. You use templates to quickly create new solutions that are based on the same design. The template contains all the solution design information, but you cannot edit a template directly or create running cases from a template.

Before you begin

Be sure to have your completed configuration checklist available.

About this task

Converting a solution to a template applies only in the development environment.

By default, new unique identifiers are created when a solution is created from the template.

Important: For most solutions, do not change the default behavior. However, if your solution contains assets that are not managed by Case Manager Builder, such as forms or search templates whose unique identifiers are referenced by programs other than IBM Case Manager, you might want to select **Include existing unique identifiers** to preserve the existing identifiers. If you preserve the existing identifiers, you cannot deploy more than one solution that is based on this template to the same target object store.

Procedure

To convert a solution to a template:

1. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   `http://server:port/navigator/?desktop=icmadmin`
   server is the IBM Content Navigator IP address or fully qualified server name.
   port is the IBM Content Navigator port number.
2. In the navigation tree in the left pane, select an object store and click **Solutions**.
3. On the Solutions page in the right pane, select the solution that you want to convert to a template.
4. Click **Actions** > **Convert to Solution Template** and complete the wizard steps.

Distributing solutions as templates

Use the IBM Case Manager administration client to distribute solution templates to your customers for further development and customization.

Before you begin

Be sure to have your completed configuration checklist available.

About this task

To distribute a solution template, use the IBM Case Manager administration client to export the solution template as a package file that can be imported into another environment. The package that you export includes all assets that were created for the solution in Case Manager Builder.

Procedure

To distribute a solution template:

1. Export the template from your source development environment.
   a. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   `http://server:port/navigator/?desktop=icmadmin`
   server is the IBM Content Navigator server name or IP address.
   port is the IBM Content Navigator port number.
   b. In the navigation tree in the left pane, select the design object store that contains the template that you want to distribute and click **Solution Templates**.
   c. On the Solution Templates page in the right pane, select the template.
   d. Click **Actions** > **Export** and complete the wizard steps.
2. Import the template into the target development environment.
   a. Start the IBM Case Manager administration client for the target development environment.
   b. In the navigation tree in the left pane, select the design object store into which you want to import the template and click **Solution Templates**.
   c. On the Solution Templates page in the right pane, click **Import** and complete the wizard steps.

What to do next

If you also want to distribute assets that were created in tools other than IBM Case Manager, package these assets by using their native tools so that you can import the assets for any solution that is created from the solution template.

Tip: To ensure that references from these other assets, such as Java programs, stored searches, and forms, to elements in the solution that are created from the template are preserved, ensure that you select the **Include existing unique identifiers** option when you convert a solution to a solution template.

In addition, distribute a comprehensive set of migration and deployment instructions that are customized for solution applications that are created from the solution template.

The process of preparing solution application assets is similar to the process used when a solution application is migrated to another environment. For more information, see "Preparing for solution migration" on page 117.

Related tasks:

"Importing a solution package by using the command line" on page 298

Unlocking solution assets

If a solution asset is locked by a user and the user cannot unlock it, for example the user is on vacation or left the company, you can unlock the asset by using the IBM Case Manager administration client.

About this task

When a user opens a solution asset for editing, the asset is locked until the user commits the updated solution. If the user cannot clear the locks by committing the solution, you can unlock the assets by using the IBM Case Manager administration client.

Attention: When you unlock an asset by using the IBM Case Manager administration client, any draft edits that were made to the asset are lost.

Procedure

To unlock an asset:

1. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   `http://server:port/navigator/?desktop=icmadmin`
   server is the IBM Content Navigator IP address or fully qualified server name.
   port is the IBM Content Navigator port number.
2. In the navigation tree in the left pane, select an object store and click **Solutions**.
3. On the Solutions page in the right pane, select the solution that contains the assets that you want to unlock and click **Actions** > **Configure** > **Locks**.
4. On the Configure locks page, select the assets to unlock and click **Unlock**.

Results

The solution asset is now unlocked and users can open and edit the asset in Case Manager Builder.

Related concepts:

Multiple user editing of solutions

Translating your case management application

You can translate the user interface elements that make up your case management application. For example, your users can then open the case management application and view it in Chinese or French by setting their browser locale to Chinese or French, or by setting the application language to Chinese or French in the Change Language and Locale Settings window.

About this task

To translate your case management application to another language, you translate all of the components of the case management application, such as the pages. For example, you can translate the My Work and Cases page titles, as shown in the following illustration:

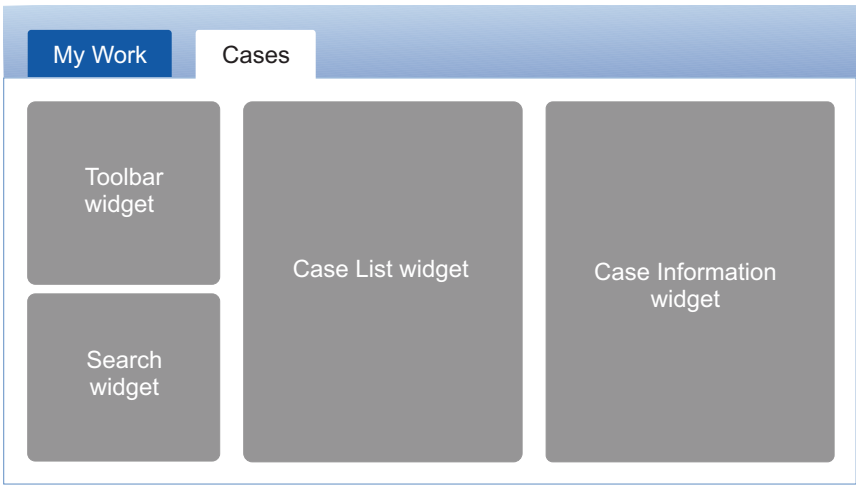


Figure 3. Default Pages

The following interface elements of the case management application cannot be translated:

- Predefined or user-created case folders, task instances, comments, solution name and description, and history entries
- Integrated inbox

When you design and create a solution, you must decide what the solution locale is. The solution locale refers to the locale of display names, such as case properties, case types, tasks, and other solution artifacts that you create with Case Manager Builder. When you deploy the solution to a target environment for the first time, you must deploy the solution under the same locale to ensure that the display names are preserved.

If you use Case Manager Builder to deploy the solution, change the browser locale.

If you use the administration client to deploy the solution, change the browser locale or change the application language value in the Change Language and Locale Settings window.

If you use the configuration tool to deploy the solution, change the JVM locale in which the configuration tool runs. Edit the `configmgr.ini` or `configmgr_cl.ini` file in the *`ICM_install_dir`*`\configure` folder and change the **`nl`** value to specify your language locale. The default value is en_US.

"Translating custom strings" on page 39

"Translating solution workflow assets that are stored in Content Platform Engine" on page 40

"Translating solution content assets that are stored in Content Platform Engine" on page 41

"Translating solution content assets that are stored in other repositories" on page 42

"Creating translated form templates for your case management application" on page 43

Related tasks:

"Defining project areas" on page 52

"Migrating the translated user interface elements of your case management application" on page 156

Translating custom strings

You can add a custom string, such as a page name, a label, or help text, to a page or a properties view. This custom string is not translated automatically. Instead, you must use a localized resource file to display the translated string for the custom string in Case Manager Client.

Before you begin

Deploy the solution before you translate the customized string. When you deploy the solution, the `nls/Resources.js` file is created or modified in the `IBM Case Manager/Solutions/`*`solution_name`* folder in the design object store or staging object store.

You can maintain and update custom translated string resources in the design object store or the staging object store depending on your organization's processes for making translated strings available to your users:

Testing, adding, and updating translated strings in a production environment only
If you test your translated strings only in a production environment and you add or update the translated custom strings for a particular language when available directly into a production environment for quick turnaround and availability. Then you can put them directly into the stage object store of the production environment with the procedure described below.

Testing, adding, and updating translated strings in a development environment first

The recommended best practice is to treat all translated custom string resources like other solution assets. Those assets should be tested and maintained in a design object store in the development environment first. Then, you move those assets to a production environment, which means that all available translated custom string resources are moved to the staging object store in the test environment. Finally, you move the complete translated solution to a production environment, which uses the design object store.

Although this procedure takes longer for the translated strings to be available in a production environment, it is the best way to maintain the solution definition, the generated default language resources, and any other manually translated custom string resources.

About this task

Default strings in pages and views are automatically translated to supported languages. The custom strings are not translated automatically, so you must add the translations for the custom strings in pages and views. Custom strings that can be translated include the following strings:

- Page titles
- Action labels and menu labels in widgets
- Title for the tabbed layout, title for the titled layout, custom property label, and property hint in views.

The translated resources are displayed based on the browser locale or the application language value in the Change Language and Locale Settings window that you use for Case Manager Client.

Procedure

To translate a custom string:

1. Using IBM Content Navigator, browse to the *design_or_staging_object_store_name*/IBM Case Manager/Solutions/*solution_name*/nls folder.
2. Download the Resources.js file.
3. Create your target locale directory in the original directory. For example, if your target locale is French, create the following directory: *design_or_staging_object_store_name*/IBM Case Manager/Solutions/*solution_name*/nls/fr. For a list of the supported non-English locales, see Planning for non-English installations. The locale values are case sensitive. Use hyphen separators instead of underscores in the locale values. For example, specify en-us instead of en_us. If your solution locale is French and you want to translate the solution to English, use locale en.
4. Edit the downloaded Resources.js file. Change the value for the custom string to the translated value for your locale. For example, change the English value for a customized page title: "New Work": "New Work" to a localized title: "New Work":"Nouveau Travail"

   Attention: The encoding of the Resources.js file must be set to UTF-8 or UTF-8 without BOM.
5. Make the same changes for any other customized strings that you want to translate.
6. Add the translated Resources.js file to the *design_or_staging_object_store_name*/IBM Case Manager/Solutions/*solution_name*/nls/fr folder as a document of Document class and as a major version. The document title must be Resources.js.
7. Repeat these steps for each language you want to translate to.
8. Redeploy the solution.

Results

When users open Case Manager Client, the translated values of customized resources display based on the browser locale or the application language value in the Change Language and Locale Settings window that you use for Case Manager Client.

Translating solution workflow assets that are stored in Content Platform Engine

You can translate your solution workflow assets that are stored in Content Platform Engine by exporting and translating an XLIFF file that contains the strings for the artifacts.

Procedure

To extract an XLIFF file by using IBM Administration Console for Content Platform Engine:

1. In the domain navigation pane, click the target object store.

2. In the object store navigation pane, click **Administrative** > **Workflow System** > **Isolated Regions** > **Isolated Region folder**.
3. On the XLIFF Configuration tab, click **New**.
4. In the New XLIFF Definition dialog box, select the **Target locale** and click **OK**.
5. Select the locale that you created and click **Download**.
6. In the Download the XLIFF File dialog box, select the source locale and click **OK**. Your browser downloads the target XLIFF file by using the strings from the source language.
7. Translate the XLIFF file.
8. Click **Upload**. Browse to the translated XLIFF file, and click **OK**. In the Upload the XLIFF File dialog box, click **OK**.
9. Repeat steps 3 - 8 for each language in which the strings are to be translated

Related information:

Creating an XLIFF file

Translating solution content assets that are stored in Content Platform Engine

You can translate the content assets of the solution that are stored in Content Platform Engine by translating the display names of case types, document types, tasks, case properties, and choice list items by using the Administration Console for Content Platform Engine.

About this task

All of the built-in Content Platform Engine content properties are translated by Content Platform Engine. Depending on the browser locale or the application language value in the Change Language and Locale Settings window, locale-sensitive system property display names are displayed in Case Manager Client.

Procedure

To translate the content artifacts, complete the following steps:

1. In Administration Console for Content Platform Engine, browse to locate the object store that contains the artifacts that you want to translate.
2. Click **Actions** and then select **Localize Class Definitions**, **Localize Property Templates**, or **Localize Choice Lists**.
3. Select a language.
4. Locate the artifacts in Administration Console for Content Platform Engine and enter localized values for the display names.

Table 3. Location of artifacts in Administration Console for Content Platform Engine

Artifact label	Location in Administration Console for Content Platform Engine
Case types	Use the Localize Class Definitions wizard under **Folder** > **Base Case** > **Case Folder**. Translate the case types that are defined in the solution.

Table 3. Location of artifacts in Administration Console for Content Platform Engine (continued)

Artifact label	Location in Administration Console for Content Platform Engine
Document types	Use the Localize Class Definitions wizard under **Document class**. If your case management application displays only the document types that are defined in a solution, you can translate only those document types. If your case management application displays all of the document types, translate all document types.
Tasks	Use the Localize Class Definitions wizard under **Task** > **Case Task**. Translate only discretionary tasks. You do not have to translate the automatic and manual task names because Case Manager Client does not display translated automatic and manual task names.
Property templates	Use the Localize Property Templates wizard. Order property templates by symbolic name. All of the case properties for a solution are displayed together in the list because they all have the same solution prefix.
Choice lists	Use the Localize Choice Lists wizard. Find all of the choice lists with the same solution prefix. Translate the display names of the choice list values. You do not have to translate the display name of the choice list.

5. Click **OK** when you are done. It might take several minutes for the changes to take effect on all nodes in the Content Platform Engine cluster.

Translating solution content assets that are stored in other repositories

You can search for and add content assets from repositories other than the case management repositories. You can translate these content assets by using the translation instructions for the repository.

About this task

If your case management environment is configured to connect to external repositories, users can add documents from the repository to a case in your case management application.

You can use IBM Content Navigator to connect to the following types of repositories:

- IBM Content Manager
- IBM Content Manager OnDemand
- IBM FileNet P8
- Repositories that support the OASIS Content Management Interoperability Services (CMIS) specification

Procedure

To translate the content artifacts from other repositories:

1. Follow the instructions for translating artifacts in the external repository that you are using.
2. In Case Manager Client, use the Change Language and Locale Settings dialog box to select the locale for your application.

3. Log out and log back in to Case Manager Client to see the artifacts in the new locale.

Creating translated form templates for your case management application

To make forms available to your users in different languages, you can create translated versions of the form templates, and then map the translated form templates to different locales in the localization proxy document which is used by your case management application.

About this task

You can create translated versions of the form templates, store the form templates in your target object store, and then map the translated form templates to different locales by using an XML file, called the localization proxy document. The localization proxy document contains the version series IDs of the translated form templates. You must configure your case management application to use the localization proxy document so that your case management application users can view and work with the forms in the language of their choice.

After you complete this task, your users can set their browser locale or the application language value in the Change Language and Locale Settings window to the language of their choice, and open the translated version of the form in the language.

Procedure

To create translated form templates and map the translated form templates to your case management application, complete the following steps:

1. If you use FileNet eForms, create translated form templates by completing the following steps:
   a. In your development environment, change the operating system locale of the FileNet eForms Designer server to the language in which you want to create a form template. For example, change your operating system to French to create a form template in French.
   b. Open FileNet eForms Designer, and then create a translated form template. If you use an existing form template, you should save the translated version of the form template in a different name. For example, you can name the translated version of a form template that is named `application` to `application_fr` or `application_french` because the translated version of the form template is in French.
2. If you use IBM Forms, follow the procedure in the IBM Forms product documentation for creating translated form templates in IBM Forms Designer. If you use an existing form template, you should save the translated version of the form template in a different name. For example, you can name the translated version of a form template that is named `application` to `application_fr` or `application_french` because the translated version of the form template is in French.
3. Add the translated version of the form template that you created in the previous step to your target object store by using IBM Content Navigator.
4. Create a localization proxy document by copying and pasting the following example text into a file with the extension `.ilp`.

```
<?xml version="1.0"?>
<localizationProxy>
     <default>
         <version>current</version>
         <id>{00F556FD-6625-462A-8880-32E00C022AA0}</id>
     </default>
     <mappings>
         <mapping locale="en-us">
             <version>current</version>
             <id>{00F556FD-6625-462A-8880-32E00C022AA0}</id>
         </mapping>
         <mapping locale="zh-cn">
             <version>released</version>
             <id>{01BF8FED-D301-4A1E-A054-519D5356F8E9}</id>
         </mapping>
         <mapping locale="fr">
             <version>released</version>
             <id>{DC5F4290-3CCF-401B-A551-60F61D182B6D}</id>
         </mapping>
     </mappings>
</localizationProxy>
```

Important: Be sure to note the behavior that is documented in Step 9: Select a localization proxy document as an attachment for the Form Attachment Work Details page. The form template that is associated with the current locale of the case worker is opened. The form data document is saved with a reference to the specific form template that was opened to create the form data. The specific form data template is used to open the form data document in subsequent steps regardless of the locale of the case worker.

Save the localization proxy document. The localization proxy document file name can be any name, but the extension must be `.ilp`.

5. In the localization proxy document, modify the following parameters:

   `version`
   The version of the form template to use. The valid values are current, released, or specific. When the version is released or current, the ID is a version series ID. When the version is specific, the ID is ID.

   A form template *vsID* or *ID* is a unique string of 32 hexadecimal characters enclosed by brackets in the following format: {xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}. For example, a form template *vsID* or *ID* might be {00F556FD-6625-462A-8880-32E00C022AA0}.

   `mapping locale`
   Maps the browser language with the template.

   The value in the `<default></default>` node is used to display a page if a mapping cannot be established by using the value in the `<mappings></mappings>` node.

   `id` The identification number of the translated form template that you created in an earlier step. In the localization proxy document, you can add as many translated form templates as you need.

   You can map from locale to sub-locale, but not from sub-locale to locale. For example, from the sample proxy document, if the browser locale is *fr* , the template with the following ID is used: {DC5F4290-3CCF-401B-A551-60F61D182B6D}. If the browser locale is *zh-cn*, the template with the following ID is used: {01BF8FED-D301-4A1E-A054-519D5356F8E9}. If the browser locale is *zh*, the default template is used.

6. Add the localization proxy document to the target object store as an object of the document class by using IBM Content Navigator. Record the identification number of the translated form template for use in a later step.
7. In Case Manager Builder, configure all Form widgets in your case management solution to use the localization proxy document:
   a. For each page that contains the Form widget, except the Form Attachment Work Details page, open the page in Page Designer and click the **Edit Settings** icon on the Form widget.
   b. Select **Form template** from the **Open the form by using** list. For **Version**, select the version of the localization proxy document to use. For **Version series ID** or **Version ID**, enter the version series ID or version ID of the localization proxy document.
   c. Save and deploy the solution.
8. Select a localization proxy document as an attachment for the Form Attachment Work Details page. The form template that is associated with the current locale of the case worker is opened. The form data document is saved with a reference to the specific form template that was opened to create the form data. The specific form data template is used to open the form data document in subsequent steps regardless of the locale of the case worker.

Related information:

Form widget

Administering your case management system

To administer your case management system, you complete tasks such as setting up project areas, monitoring system performance, and modifying systemwide configurations. You can also back up, restore, or tune the system.

Restarting components in a single-server IBM Case Manager environment

Server maintenance and software updates sometimes require a server reboot. You must manually restart the components in your IBM Case Manager environment on an AIX or Linux server. On a Windows server, the components restart automatically.

About this task

If your single-server IBM Case Manager environment is installed on a Windows server, all your components and applications restart automatically after a reboot.

You must have the passwords for your components and applications in order to complete the restart steps.

Procedure

To start IBM Case Manager components:

1. Log in as the root user.
2. Restart the database. For example, restart DB2® by entering the following command: `su - dsrdbm01 -c db2start`
3. Start the LDAP server. For example, to start Tivoli® Directory Server:
   a. Change to the Tivoli Directory Server directory by entering the following command: `cd /opt/ibm/ldap/V6.3/bin`
   b. Start Tivoli Directory Server by entering the following command: `./ibmdirctl -h localhost -D cn=root -w` *`password`* `start`
   c. Make sure that Tivoli Directory Server is running by entering the following command: `./ibmdirctl -h localhost -D cn=root -w` *`password`* `status`
4. Start the web application server.
   a. Change to the *`profile_root`*`/bin` directory. *profile_root* is the directory path that contains your profile, for example: `/opt/ibm/WebSphere/AppServer/profiles/AppSrv01`.
   b. Run the following command:

      ```
      ./startServer.sh server1
      ```

Starting your system

You might need to restart your system for server maintenance or software updates. You must manually start components in your IBM Case Manager environment on an AIX, Linux, or Linux for System z server.

About this task

If you have a single-server IBM Case Manager environment that is installed on a Windows server, all of your components and applications restart automatically.

You must have the passwords for your components and applications to complete the steps.

Procedure

To start IBM Case Manager components:

1. Log in as the root user.
2. Start DB2 by entering the following command: `su - dsrdbm01 -c db2start`
3. Start Tivoli Directory Server:
   a. Change to the Tivoli Directory Server directory by entering the following command: `cd /opt/ibm/ldap/V6.3/bin`
   b. Start Tivoli Directory Server by entering the following command: `./ibmdirctl -h localhost -D cn=root -w` *`password`* `start`
   c. Make sure that Tivoli Directory Server is running by entering the following command: `./ibmdirctl -h localhost -D cn=root -w` *`password`* `status`
4. Start the web application server.

Web application server	Startup procedure
WebSphere Application Server	1. Change to the *`profile_root`*`/bin` directory. *profile_root* is the directory path that contains your profile, for example: `/opt/ibm/WebSphere/AppServer`. 2. Run the following command: `./startServer.sh server1`

Web application server	Startup procedure

Oracle WebLogic Server	1. Change to the *domain_root*/bin directory. *domain_root* is the root directory of the domain, for example: /opt/Oracle/Middleware/user_projects/domains/*domain_name*.
	2. Run the following command:
	`startWeblogic.sh`
	
	By default, logs are displayed in a console window. To save logs in a file, use the nohup command:
	`nohup ./startWebLogic.sh >>log_file_name.log 2>&1 &`
	
	Tip: To avoid being prompted to log in every time you start Oracle WebLogic Server, create a file called boot.properties that contains the following lines:
	`username=web_admin_user_name`
	`password=user_password`
	
	Save the boot.properties file in the *domain_root*/AdminServer/security directory. When you restart Oracle WebLogic Server, the user name and password will be encrypted and displayed as in this example:
	`username=`
	`{AES}JmzKfE4sQj+lbKwnn8KC0BwfQNTU9+az1KFZBiN4b0M\=`
	`password=`
	`{AES}K9BgKir2ETOR1Or+r7KyfW+qf0saALa4zlBh1M8zMUM\=`

Shutting down your system

You might need to shut down your system for server maintenance or software updates.

Procedure

To shut down IBM Case Manager:

Stop the web application server. In a distributed system architecture, first shut down the nodes, and then shut down the main server.

Web application server	Shutdown procedure
WebSphere Application Server	1. Change to the *profile_root*/bin directory. *profile_root* is the directory that contains your profile, for example: /opt/ibm/WebSphere/AppServer. 2. Run the command to shut down the server: Windows: stopServer.bat server1 AIX, Linux, and Linux for System z: ./stopServer.sh server1 If global security is enabled, you must specify a user name and password for authentication. You can wait to be prompted for the user name and password, or append the following options to the stopServer command: -username *user_name* -password *password*
Oracle WebLogic Server	1. Change to the *domain_root*/bin directory. *domain_root* is the root directory of the domain, for example: /opt/Oracle/Middleware/user_projects/domains/*domain_name*. 2. Run the command to shut down the server: Windows: stopWeblogic.cmd AIX, Linux, and Linux for System z: ./stopWeblogic.sh

Setting up project areas

You use project areas to limit the effects of resetting the test environment to other users working on other projects in the same development environment.

About this task

Because you might have multiple people working in the development environment on multiple projects, you can define project areas to limit the effects of resetting the test environment. The design object store can have multiple project areas, and each project area corresponds to one test environment. When you have project areas set up and you reset the test environment from Case Manager Builder, only a single project area is reset. The entire design object store is not affected, and other Case Manager Builder users who are working on solutions in the same design object store can continue working without interruption.

For example, you might be a solution provider and have a credit card processing solution that is ready to test, but you also have an insurance solution in your development environment that is still under development. You can assign the credit card processing solution to a project area so that you can reset the test environment when you are done testing and you will not interrupt work on the insurance solution that is in development.

You can assign specific solutions and users to each project area. Each user can belong only to one project area and the default project area. Users can define and modify solutions only in the project area that they are assigned to. Users who are not assigned to a project area cannot log into Case Manager Builder. Users with access to the IBM Case Manager development system are automatically assigned to the default project area.

Each development environment requires a default project area that is named dev_env_connection_definition. You can define more project areas as needed. As you work with project areas, note the following differences between the required default project area and regular project areas:

- You can enter your own connection definition name when you define a regular project area, but the default project area has a predefined connection definition name that you cannot change.
- You can assign user groups to the default project area, but you can only assign individual users to a regular project area. A user can be assigned to one regular project area only, in addition to the default project area.
- When a user logs on to Case Manager Builder, the user will automatically go to the regular project area that they are assigned to. If you want the user to go directly to the default project area when they log on to Case Manager Builder, you must remove the user from the regular project area.

If you used FileNet Deployment Manager to import a solution, the solution is assigned to a default project area and you will not see the solution in Case Manager Builder. You can use the IBM Case Manager administration client, or the Manage Project Areas wizard in the IBM Case Manager configuration tool, to assign the solution to your preferred project area.

"Creating a target object store"

"Defining project areas" on page 52

"Managing project areas" on page 53

Creating a target object store

You must create a target object store for each project area.

Before you begin

Prepare appropriate users and groups to assign in the object store creation wizard. For more information, see Planning for security in the development environment.

Procedure

To create a target object store for a project area:

1. Create an object store in IBM FileNet P8. For more information, see Defining object stores and Creating an object store.

   Tip: In the object store creation wizard, on the page where you specify the add-ons to install, click **Workplace/WorkplaceXT Configuration** to select the add-ons that are required by IBM Case Manager.
2. If you have not already created a workflow system to contain isolated regions, create one now. For more information, see Creating a workflow system.
3. Convert the object store to a case management target object store.
   a. Start the IBM Case Manager administration client. Enter the following URL in a browser:

`http://server:port/navigator/?desktop=icmadmin`
server is the IBM Content Navigator server name or IP address.
port is the IBM Content Navigator port number.

b. In the navigation tree in the left pane, right-click the object store, select **Convert to Target Object Store**, and complete the wizard steps.

What to do next

After you create the target object store, you can define and register the project area. If you plan to use the Timeline Visualizer widget to view case history for your project area, set up a case history store.

Related tasks:

"Preparing a database for the case history store" on page 61

Defining project areas

You can define new, nondefault project areas, assign solutions and users to a project area, and remove project areas.

Before you begin

Be sure to have your completed configuration checklist available.

About this task

You can define project areas for the development environment by using the IBM Case Manager administration client. After you define a project area, you must register it before you can use it.

Restriction: Each project area requires a unique connection point, and only one connection point can be associated with a target object store.

Procedure

To define a new project area:

1. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   `http://server:port/navigator/?desktop=icmadmin`
   server is the IBM Content Navigator IP address or fully qualified server name.
   port is the IBM Content Navigator port number.
2. In the navigation tree in the left pane, select a design object store and click **Project Areas**.
3. On the Project Areas page in the right pane, click **Define** and complete the wizard steps.
4. Register the project area.
   a. On the Project Areas page in the right pane, select the project area to register.
   b. Click **Actions** > **Register** and complete the wizard steps.

What to do next

Set security for the project area users.

Related tasks:

"Defining and modifying project areas by using the command line" on page 284

Related reference:

Configuration checklist

Related information:

Planning for project areas

Managing project areas

Manage project areas and users so that users who are working on different projects in the same environment can do so without interruption.

About this task

If you have many solution projects in different phases of development, you can define a project area for each solution so that when a solution is ready to test, you can do so without affecting the other solutions that share the same design object store. You can use the IBM Case Manager administration client to define project areas, remove project areas, move solutions to different project areas, and add or remove users from project areas.

Restriction: Each project area requires a unique connection point, and only one connection point can be associated with an object store.

Procedure

To manage your project areas:

1. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   `http://server:port/navigator/?desktop=icmadmin`
   server is the IBM Content Navigator IP address or fully qualified server name.
   port is the IBM Content Navigator port number.
2. In the navigation tree in the left pane, select a design object store and click **Project Areas**.
3. On the Project Areas page in the right pane, select a project area and click **Actions** to edit, register, or delete the project area.

   Restriction:

   - You cannot delete the default project area; you can delete regular project areas only.
   - For the default project area, you can add and remove users and groups. For regular project areas, you can add and remove individual users only.
   - You can add a user to one regular project area only, in addition to the default project area.
   - If you add a solution to a project area and that solution does not match the integration type of the project area, the solution is filtered out.
   - If you remove a solution from a project area other than the default project area, that solution is assigned automatically to the default project area. However, if the default project area is of a different integration type than the solution, then the system prevents you from removing that solution from the non-default project area.

Setting up target environments

Setting up the target environment includes creating the target object store, creating a workflow system, and running tasks in the IBM Case Manager configuration tool or administration client to define and register the target environment. Depending on the solutions that you plan to deploy in the target environment, you might need to run additional configuration tasks.

About this task

In test and production environments, you deploy solutions in target environments. The first time that you run the configuration tool to configure the production environment after you install IBM Case Manager, you must define and register at least one target environment. Later, you can use the administration client to define additional target environments iteratively as needed to support your solutions.

You can deploy one solution or many solutions into a single target environment. Ensure that you have enough system resources for the number of cases that you anticipate having in each database.

For the simplest configuration, deploy all of your solutions in a single target environment. In this configuration, all of the solutions share a single Content Platform Engine target object store and a single workflow system.

To separate the workload among databases, you can deploy each solution or a few solutions into a separate target environment. In this configuration, each solution or group of solutions is provided with a dedicated Content Platform Engine target object store and workflow system. This configuration provides data separation between the solutions, which allows for greater flexibility in database operations, database maintenance, and assigning security privileges.

If you configure multiple test and production environments, and you configure multiple IBM FileNet P8 domains, ensure that each target environment is on the same domain as its corresponding staging object store.

Security considerations: The LDAP security configuration for solutions in a production environment is more restricted than the development environment. Production environments can use a different LDAP than the development environment. The LDAP is tied to the FileNet P8 domain that hosts the IBM Case Manager production domain.

It is a best practice to create a case management master group to use for assigning access to object stores at the time that you create the object store. Give this group **Use object store** permission. You can grant new users access to the object store by adding them to the master group. This approach can prevent issues with changing security on an established object store. For more information, see Planning for security in the production environment.

"Creating or upgrading a target object store for test or production environments" on page 55

"Creating custom desktops" on page 56

"Defining and registering target environments" on page 57

"Managing target environment definitions" on page 58

Related tasks:

"Configuring the target environment after solution deployment" on page 153

Creating or upgrading a target object store for test or production environments

A target object store is required for each target environment in the test and production domains.

Before you begin

Prepare appropriate users and groups to assign in the object store creation wizard. It is a best practice to create a case management master group to use for assigning access to object stores at the time that you create the object store. Give this group **Use object store** permission. With this method, you can grant new users access to the object store by adding them to the master group. This approach can prevent issues with changing security on an established object store. For information, see Planning for security in the production environment.

About this task

A target object store contains the following artifacts for a deployed solution:

- Deployed solution folder: A folder structure for a deployed solution in the target object store. Case instances are created under this structure.
- Case class: A representation for a case type in a solution.
- Document class: A definition of a document type.
- Property template: A definition of a property type.
- Task class: A definition of a task type.
- Subscription: A case or task event condition to corresponding Content Platform Engine event actions.

Procedure

To create or upgrade a target object store for your test or production environment:

1. For a new target environment, if you did not previously create an object store, create one in IBM FileNet P8. For information, see Defining object stores and Creating an object store.
2. For a new target environment, if you did not previously create a workflow system, create one now. For information, see Creating a workflow system.
3. For a new target environment or an upgraded target environment, convert the object store to a case management target object store.
   a. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   `http://server:port/navigator/?desktop=icmadmin`
   server is the IBM Content Navigator server name or IP address.
   port is the IBM Content Navigator port number.
   b. In the navigation tree in the left pane, right-click the object store, select **Convert to Target Object Store**, and complete the wizard steps.

What to do next

Do the following tasks after you create or upgrade the target object store:

1. Define and register the target environment. See "Defining and registering target environments" on page 57.
2. Optional: If you plan to use the Timeline Visualizer widget to view case history in the solutions that you deploy to this target environment, set up a case

history store before you migrate and deploy the solutions. See “Preparing a database for the case history store” on page 61 and Timeline Visualizer widget.

3. Optional: If you plan to use the IBM Case Monitor Dashboard to view business activity data for cases and tasks in the solutions that you deploy to this target environment, set up a Case Analyzer store before you migrate and deploy the solutions.
4. Configure indexes for the target object store indexes. See Configuring production target object store indexes.

Creating custom desktops

You can use extra desktops in IBM Content Navigator to group target environments and solutions. This approach makes it possible to separate groups of solution users that are based on roles, organizations, or location.

About this task

If you plan to use separate desktops to group target environments, you can create the desktops before you define and register the environment. Then, you can specify the custom desktops as part of the define and registration tasks.

Use IBM Content Navigator to define as many desktops as your planned environment requires.

When you register a target environment, the target object store repository is added both to the specified desktop and to the master IBM Content Navigator desktop for IBM Case Manager, icm.

Procedure

To create a custom desktop to use with IBM Case Manager:

1. Define a new desktop in the IBM Content Navigator web client administration feature. For the authentication repository, specify a repository for the Content Platform Engine domain that you are using for your IBM Case Manager environment.
2. Use the tasks for defining and registering your target environments to add the desktop to your target environment.

What to do next

Define and register your target environments. If you want to use the IBM Case Manager administration client on your custom desktop, use IBM Content Navigator to add that feature to your desktop. You can also create a desktop that includes the administration client feature without associating target environments with that desktop, if the authentication repository is a FileNet P8 object store from the correct domain. You can also further customize your desktop by using IBM Content Navigator functions, such as restricting access to the desktop to a specific list of users or applying a theme to control the colors and images that display in the interface.

Related information:

Defining desktops

Defining and registering target environments

You can define target environments for a test environment or production environment by using the IBM Case Manager configuration tool or the IBM Case Manager administration client. After you define a target environment definition, you must register it before you can use it.

Before you begin

You must create and configure a case management object store before you define a target environment.

About this task

The first time that you run the configuration tool to configure the production environment after you install IBM Case Manager, you must define at least one target environment. Later, you can use the administration client to define more target environments as needed to support your solutions.

A *target environment definition* specifies the target environment to which an IBM Case Manager solution is deployed. It contains information about the connection point and a logical to physical page mapping. By using the connection point, IBM Case Manager can discover the target object store and isolated region number.

When you define a target environment, you select the connection point for the target object store. Multiple connection points for the same target object store can exist. If required to support solutions that you upgrade to IBM Case Manager V5.2, multiple target environments can share the same connection point.

When you register a target environment, you select the Case Manager Client desktop that you want to use to access solutions that are hosted in the target environment. You also specify credentials for the user ID that you want to use to run workflows for case operations.

Procedure

To define and register a new target environment by using the configuration tool:

1. Enter the appropriate command for your environment:

Option	Description
AIX Linux Linux for System z	1. Change to the *install_path*/configure directory. *install_path* is the location where IBM Case Manager is installed, for example, /opt/IBM/CaseManagement. 2. Run the following command: ./configmgr

Option	Description
Windows	Perform one of the following actions: • Click **Start** > **All Programs** > **IBM Case Manager** > **Case Manager Configuration Tool**. • Run the following command: *install_path*\configure\configmgr.exe *install_path* is the location where IBM Case Manager is installed, for example, C:\Program Files\IBM\CaseManagement for a fresh install or C:\Program Files (x86)\IBM\CaseManagement for an upgrade.

2. Click **File** > **Open profile** and select a production environment profile.
3. After the list of configuration tasks is displayed, edit, save, and run the following tasks:
   - Define Target Environment
   - Register Target Environment

To define and register a new target environment by using the administration client:

4. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   http://*server*:*port*/navigator/?desktop=icmadmin
   server is the IBM Content Navigator IP address or fully qualified server name.
   port is the IBM Content Navigator port number.
5. From the list of object stores in the navigation tree in the left pane, select a staging object store to open it. Click **Target Environments**.
6. On the Target Environments page in the right pane, click **Define** and complete the wizard steps.
7. Register the target environment:
   a. On the Target Environments page in the right pane, select the target environment that you want to register.
   b. Click **Actions** > **Register** and complete the wizard steps.

What to do next

Depending on the assets in the solution or solutions that you plan to deploy in this target environment, you might need to run the following configuration tasks. To run these tasks, you must use the configuration tool:

- Configure IBM Content Manager Host Properties
- Configure IBM Business Process Manager
- Configure Business Rules
- Register the External Data Service

Related information:

"IBM Case Manager configuration tool task fails with 414 error" on page 205

Managing target environment definitions

Use the IBM Case Manager administration client to view and edit properties that were defined for a target environment or to delete a target environment definition.

Procedure

To manage target environment definitions:

1. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   `http://server:port/navigator/?desktop=icmadmin`
   server is the IBM Content Navigator IP address or fully qualified server name. *port* is the IBM Content Navigator port number.
2. In the navigation tree in the left pane, select a staging object store to open it. Click to expand **Target Environments**.
3. On the Target Environments page in the right pane, select a target environment definition and click **Actions** > **View and Edit**. Complete the wizard steps. Only the properties that you can change are available for editing.

   You can also click **Actions** > **Delete** to delete the target environment definition. You cannot delete all target environment definitions; at least one target environment must be defined in your production environment profile.

Enabling and disabling plug-ins for the IBM Case Manager desktop

IBM Case Manager loads selected plug-ins by default for the Case Manager desktop and Case Manager administration desktop. You can configure these desktops in the IBM Content Navigator administration desktop to change the plug-ins that are available for the desktop.

About this task

Previously, IBM Content Navigator loaded all plug-ins, even if a plug-in was not needed for the layout or features included in a desktop. IBM Content Navigator displays the registered plug-ins so that you can enable all plug-ins for the desktop or select only the plug-ins that are needed.

For IBM Case Manager, the following plug-ins are available to be loaded:

IBM Case Manager API plug-in
: Load this plug-in to provide API support for Case Manager Client, IBM Case Manager Monitor Dashboard, and the IBM Case Manager Box event listener.

IBM Case Manager client plug-in
: Load this plug-in to enable Case Manager Client in IBM Content Navigator. This plug-in also supports the IBM Case Manager Dashboard plug-in.

IBM Case Manager administration plug-in
: Load this plug-in to enable the IBM Case Manager administration client in IBM Content Navigator.

IBM Case Manager custom plug-ins
: Load any plug-ins that are required to enable any custom widget packages or extension packages that you use with IBM Case Manager.

IBM Case Manager Mobile Configurator
: Load this plug-in to enable the configurator that is required if you are using the IBM Case Manager Mobile app.

IBM Case Manager Box Event Listener plug-in
: Load this plug-in to enable the Box event listener in IBM Content Navigator.

IBM Case Dashboard plug-in
Load this plug-in to enable IBM Case Monitor Dashboard in IBM Content Navigator.

Content Platform Engine Applets Support
Load this plug-in to enable Process Designer to be used with IBM Case Manager.

Important: If the ICMAdminClientPlugin feature was manually added to the Case Manager desktop, you must add this plug-in to be loaded.

By default, the IBM Case Manager configuration tool selects the following plug-ins to be loaded for the Case Manager desktop:

- IBM Case Manager API plug-in
- IBM Case Manager client plug-in
- IBM Case Manager custom plug-in
- Content Platform Engine Applets Support plug-in

The IBM Case Manager configuration tool selects the IBM Case Manager administration plug-in to be loaded for the Case Manager administration desktop. If Box collaboration is enabled, the configuration tool also selects the IBM Case Manager API plug-in and IBM Case Manager Box Event Listener plug-in to be loaded.

By default, the IBM Case Manager configuration tool selects the following plug-ins to be loaded for the IBM Case Monitor desktop:

- IBM Case Manager API plug-in
- IBM Case Manager client plug-in
- IBM Case Dashboard plug-in

You can configure the desktop to disable one or more of plug-ins or to enable other plug-ins for use with the IBM Case Manager desktop or IBM Case Manager administration desktop.

The IBM Case Manager configuration tool does not affect the plug-ins that are loaded for a custom desktop.

Procedure

To enable or disable a plug-in for the IBM Case Manager desktop:

1. Log in to IBM Content Navigator as an administrator. Enter the following URL in a browser:

   `http://server:port/navigator`

   server is the IBM Content Navigator server name or IP address.

   port is the IBM Content Navigator port number.
2. Navigate to **Desktops** > **Case Manager** > **General**.
3. In the **Plug-ins** area, select **Select the deployed plug-ins to enable for use with this desktop**. Then, select the plug-ins that you want loaded for the IBM Case Manager desktop and clear the check box for any plug-in that you do not want loaded.

What to do next

After you enable or disable plug-ins for a desktop, ensure that the desktop works as expected. For example, ensure that Case Manager Client works correctly with the Content Platform Engine Support Applets plug-in that is used to host Process Designer and with any custom widgets packages.

Enabling favorites and sync

Users can create favorites to quickly find the items that they work with frequently. When a user creates a favorite, they can optionally choose to sync the item to their workstation or device so that they always have the latest version of the document available. To enable these features, you must install a sync client and configure settings in the IBM Content Navigator administration desktop.

Preparing a database for the case history store

If you plan to use the Timeline Visualizer widget to view case history over time, you must prepare a database to record extended case history data.

About this task

The system can store extended case history data in the database instance that is used for the target object store, or in a separate database instance. Consider the capacity of your database server, the case size, and the case load when determining where to store extended case history data.

When extended case history data is stored in the database instance that is used for the target object store, you do not need to define an additional JDBC data source, and you can easily back up the case history store along with the target object store. However, including the case history data increases the load on the database server, and this can have a negative impact on performance. Defining a separate database on the same remote database server as the target object store can also degrade performance.

Alternatively, the system can store extended case history data in a separate database instance. For example, you might want to use a separate, remote database server if I/O throughput is problematic. If the system stores extended case history data on a different remote database server, you can get additional disk arms, disk space, CPU, and memory to support it.

Restriction: You cannot delete cases or prune extended case history data. Ensure that there is sufficient disk space to store extended case history data.

The following procedure refers to IBM FileNet P8 tools and procedures to set up a database for your case history store.

Procedure

To store extended case history in a separate database instance:

1. Prepare the database for the case history store. For more information, see Database administrator installation tasks.
2. Create JDBC data sources. Run the Configure JDBC Data Sources task by using the IBM FileNet P8 Configuration Manager. For more information, see Editing the Configure JDBC Data Sources tasks and Configuration Manager reference.

3. Create a database connection. For more information, see Creating a database connection. Based on performance considerations, you might want to share data sources. For more information, see Sharing data sources. You enter the database schema name when you configure and enable the case history store by using the IBM Case Manager administration client.

What to do next

Select custom properties to audit and enable the case history store by using the IBM Case Manager administration client.

Related tasks:

"Configuring auditing" on page 21

Monitoring system performance

Monitor the performance of IBM Case Manager by using IBM System Dashboard for Enterprise Content Management.

The System Dashboard for Enterprise Content Management displays real-time performance data that you can use to proactively identify and resolve potential performance problems before they occur. The performance data can also be archived for management reporting and trend analysis.

As the administrator, you monitor work items, case tasks, and other processes that run in the background, and if they fail to launch, you need to manually intervene to recover them. If a workflow is in the malfunction state, the work item will be sent to either the predefined Malfunction submap or a user-defined malfunction submap. You can use Process Administrator to monitor the Conductor queue (for the predefined Malfunction map, configured by default) or your customized malfunction queue.

The solution can have an IT administrator role with access to Content Platform Engine tools. The IT administrator can use either Process Administrator or Process Tracker to move the work items out of the malfunction state.

See the IBM FileNet P8 documentation for instructions on installing, configuring, and using the System Dashboard for Enterprise Content Management, as well as for retrieving queued items in the malfunction state.

"IBM Case Manager counters"

Related information:

- Using the IBM System Dashboard for Enterprise Content Management
- IBM Case Manager counters
- About system maps (including the Malfunction map)
- Creating a component queue

IBM Case Manager counters

Counters for IBM Case Manager include REST API groups and counters, Java API groups and counters, and Deployment groups and counters.

"REST API groups and counters" on page 63

"Java API groups and counters" on page 64

"Event handler counters" on page 64

REST API groups and counters

Groups

Property	Description
GET	REST API that requests a representation of the specified resource.
DELETE	REST API that deletes a specified resource.
POST	REST API that submits data to be processed to the identified resource.
PUT	REST API that uploads a representation of the specified resource.

Counters

Property	Counter Type	Description
Cases	Event	Manually create a case instance of a case type.
Cases	Duration	Manually create a case instance of a case type.
Case Instance	Event	Retrieve, update, or split a case instance.
Case Instance	Duration	Retrieve, update, or split a case instance.
Case Type	Event	Get the information about a case type.
Case Type	Duration	Get the information about a case type.
Case Comments	Event	Return or create comments of a specific type for a case instance.
Case Comments	Duration	Return or create comments of a specific type for a case instance.
Case History	Event	Return a filtered case history of a case instance.
Case History	Duration	Return a filtered case history of a case instance.
Case Tasks	Event	Lists task instances of a case instance.
Case Tasks	Duration	Lists task instances of a case instance.
Case Task Type	Event	Get the information about a case type.
Case Task Type	Duration	Get the information about a case type.
Case Status	Event	Return the status of a case instance.
Case Status	Duration	Return the status of a case instance.
Related Cases	Event	Return all of the related cases (of any type) of a case instance.
Related Cases	Duration	Return all of the related cases (of any type) of a case instance.
Solution Deployment	Event	Starts asynchronous solution deployment or retrieves solution information.
Solution Deployment	Duration	Starts asynchronous solution deployment or retrieves solution information.
Solution	Event	Copy a solution in the design object store.
Solution	Duration	Copy a solution in the design object store.
Discretionary Task Types	Event	Return a list of the discretionary tasks for a case worker.
Discretionary Task Types	Duration	Return a list of the discretionary tasks for a case worker.

Counters

Property	Counter Type	Description
Document Class	Event	Return the information of a document class.
Document Class	Duration	Return the information of a document class.
Document Classes	Event	Return the list of document classes in the target object store.
Document Classes	Duration	Return the list of document classes in the target object store.
Task Instance	Event	Change the state of an instance of a task.
Task Instance	Duration	Change the state of an instance of a task.

Java API groups and counters

Groups

Property	Description
API	Placeholder for all API-related PCH counters.

Counters

Property	Counter Type	Description
Case History Query	Duration	Fetching case history of all types.
Create New Case	Event	Create a case instance by using the Java API.
Create New Case	Duration	Create a case instance by using the Java API.
Start Task	Event	Manually start a task instance (moving from ready to working).
Start Task	Duration	Manually start a task instance (moving from ready to working).
Create Task	Event	Create a task instance by using the Java API.
Create Task	Duration	Create a task instance by using the Java API.

Event handler counters

Property	Type	Description
Start Automatic Task	Event	Start an automatic (system) task (move from ready to working).
Task state that is changed to WORKING	Event	An object state task is changed from ready to working.
Task state that is changed to COMPLETED	Event	An object state task is changed from working to completed.
Task state that is changed to FAILED	Event	An object state task is changed from working to failed.

Deployment groups and counters

Groups

Property	Description
Deployment	Placeholder for all IBM Case Manager deployment-related PCH counters.

Counters

Property	Counter Type	Description
Deployed Document Types	Meter	Number of document types that are deployed for a solution.
Deployed Document Types	Duration	Number of document types that are deployed for a solution.
Deployed Case Types	Meter	Number of case types that are deployed for a solution.
Deployed Case Types	Duration	Number of case types that are deployed for a solution.
Deployed Task Types	Meter	Number of document types that are deployed for a solution.
Deployed Task Types	Duration	Number of document types that are deployed for a solution.
Deployed Property Definitions	Meter	Number of property definitions that are deployed for a solution.
Deployed Property Definitions	Duration	Number of property definitions that are deployed for a solution.
Deployed Property Templates	Meter	Number of property templates that are deployed for a solution.
Deployed Property Templates	Duration	Number of property templates that are deployed for a solution.
Choice Lists	Meter	Number of choice lists that are deployed for a solution.
Choice Lists	Duration	Number of choice lists that are deployed for a solution.

Plug-in Service counters

Plug-in Service counters

Property	Counter Type	Description
CaseBoxService_createCollaboration	Duration	Service to create a Box collaboration folder
CaseBoxService_getCollaborators	Duration	Service to get the users who are invited to a Box collaboration folder
CaseBoxService_retrieveBoxUser	Duration	Service to get the identifier for a specific Box user
CaseBoxService_searchBoxGroups	Duration	Service to search Box groups
CaseBoxService_searchBoxUsers	Duration	Service to search Box users
CaseBoxService_searchBoxUsersGroups	Duration	Service to search Box users and groups
CaseBoxService_submitRequest	Duration	Service to submit a request to Box
CaseBoxService_updateCollaborators	Duration	Service to update the users who are invited to a Box collaboration folder

Plug-in Service counters

Property	Counter Type	Description
CaseCommentService	Event	Service invoked to add and retrieve comments
CaseCommentService	Duration	Service invoked to add and retrieve comments
CaseHistoryConfigurationStatus	Event	Service to get the configuration status of the case history feature
CaseHistoryConfigurationStatus	Duration	Service to get the configuration status of the case history feature
CaseHistoryEventsService	Event	Timevisualizer-specific service
CaseHistoryEventsService	Duration	Timevisualizer-specific service
CaseHistoryNamedSnapshotPostService	Event	Timevisualizer-specific service
CaseHistoryNamedSnapshotPostService	Duration	Timevisualizer-specific service
CaseHistoryNamedSnapshotDeleteService	Event	Timevisualizer-specific service
CaseHistoryNamedSnapshotDeleteService	Duration	Timevisualizer-specific service
CaseHistoryNamedSnapshotsService	Event	Timevisualizer-specific service
CaseHistoryNamedSnapshotsService	Duration	Timevisualizer-specific service
CaseHistoryNextEventsService	Event	Timevisualizer-specific service
CaseHistoryNextEventsService	Duration	Timevisualizer-specific service
CaseHistoryNamedNonTaskEventsService	Event	Timevisualizer-specific service
CaseHistoryNamedNonTaskEventsService	Duration	Timevisualizer-specific service
CaseHistoryOverviewService	Event	Timevisualizer-specific service
CaseHistoryOverviewService	Duration	Timevisualizer-specific service
CaseHistorySnapshotDetailsService	Event	Timevisualizer-specific service
CaseHistorySnapshotDetailsService	Duration	Timevisualizer-specific service
CaseHistorySnapshotEntitiesService	Event	Timevisualizer-specific service
CaseHistorySnapshotEntitiesService	Duration	Timevisualizer-specific service
CaseHistorySnapshotTaskStepsService	Event	Timevisualizer-specific service
CaseHistorySnapshotTaskStepsService	Duration	Timevisualizer-specific service
CaseHistoryStepsEventsService	Event	Timevisualizer-specific service
CaseHistoryStepsEventsService	Duration	Timevisualizer-specific service
CaseHistoryTasksEventsService	Event	Timevisualizer-specific service
CaseHistoryTasksEventsService	Duration	Timevisualizer-specific service
CaseHistoryTasksService	Event	Timevisualizer-specific service
CaseHistoryTasksService	Duration	Timevisualizer-specific service
CaseHistoryTasksStepsService	Event	Timevisualizer-specific service
CaseHistoryTasksStepsService	Duration	Timevisualizer-specific service
CaseService	Event	Service to retrieve, create, update, save, relate/unrelate, and split a case instance
CaseService	Duration	Service to retrieve, create, update, save, relate/unrelate, and split a case instance
ConfigurationService	Event	Service to load or update the user configuration
ConfigurationService	Duration	Service to load or update the user configuration
DiscretionaryTaskService	Event	Service to create discretionary tasks

Plug-in Service counters

Property	Counter Type	Description
DiscretionaryTaskService	Duration	Service to create discretionary tasks
DynamicTaskService	Event	Service to create or retrieve custom tasks
DynamicTaskService	Duration	Service to create or retrieve custom tasks
ExternalDocumentReferenceService	Event	Service to get or add external document references
ExternalDocumentReferenceService	Duration	Service to get or add external document references
GetCaseHistoryService	Event	Service to get the case history
GetCaseHistoryService	Duration	Service to get the case history
GetCaseTasksService	Event	Service to get the list of tasks in a case instance
GetCaseTasksService	Duration	Service to get the list of tasks in a case instance
GetCaseTypePageService	Event	Service to get the page information for a specific case type
GetCaseTypePageService	Duration	Service to get the page information for a specific case type
GetCaseTypePropertiesService	Event	Service to get the case type properties
GetCaseTypePropertiesService	Duration	Service to get the case type properties
GetCaseTypeService	Event	Service to get a case type
GetCaseTypeService	Duration	Service to get a case type
GetMC8ProxyFolderPIDService	Event	Service to get the CM8 proxy folder PID
GetMC8ProxyFolderPIDService	Duration	Service to get the CM8 proxy folder PID
GetDiscretionaryTaskTypesService	Event	Service to get the discretionary task types
GetDiscretionaryTaskTypesService	Duration	Service to get the discretionary task types
GetDocumentTypesService	Event	Service to get the document types
GetDocumentTypesService	Duration	Service to get the document types
GetDocumentTasksService	Event	Service to get the existing dynamic tasks
GetDocumentTasksService	Duration	Service to get the existing dynamic tasks
GetRoleMembersService	Event	Service to get the members of a role
GetRoleMembersService	Duration	Service to get the members of a role
GetSolutionInformationService	Event	Service to get the document types
GetSolutionInformationService	Duration	Service to get the document types
GetSolutionListService	Event	Service to get the list of solutions
GetSolutionListService	Duration	Service to get the list of solutions
GetSolutionStaticPagesService	Event	Service to get the static pages for a solution
GetSolutionStaticPagesService	Duration	Service to get the static pages for a solution
GetTaskMileStonesService	Event	Service to get a task milestone
GetTaskMileStonesService	Duration	Service to get a task milestone
RelatedCasesService	Event	Service to get the cases related to another case
RelatedCasesService	Duration	Service to get the cases related to another case
RunCEQueryService	Event	Internal service
RunCEQueryService	Duration	Internal service
SearchCaseTasksService	Event	Service to search for tasks within a case

Plug-in Service counters

Property	Counter Type	Description
SearchCaseTasksService	Duration	Service to search for tasks within a case
StepElementService	Event	Service to get, create, update, save work items
StepElementService	Duration	Service to get, create, update, save work items
TaskService	Event	Service to get, enable disable, start, stop, restart and complete a task
TaskService	Duration	Service to get, enable disable, start, stop, restart and complete a task
UpdatingBatchService	Event	Service to execute batch operations
UpdatingBatchService	Duration	Service to execute batch operations

ICMBoxPlug-in Service counters

ICMBoxPlug-in Service counters

Property	Counter Type	Description
CaseBoxEventsListener_Initiation	Duration	Service invoked to initiate the Box event listener
CaseBoxEventsListener_ServerTokenLogin	Duration	Service invoked to log in to Box by using the server token.
*handler name*_**HandlerInvocation**	Duration	Service invoked to invoke the specified event handler.

Backing up your system

It is a best practice to periodically back up the IBM Case Manager system so that you can more rapidly recover from the loss of data. Creating a backup policy requires familiarity with the backup requirements of all system components.

About this task

When you create a backup policy for your IBM Case Manager system, you must be familiar with the requirements of all of the components. For example, the IBM FileNet P8 contains both content and workflow elements for the system. You must use the information from the FileNet P8 documentation to understand and plan for your backups of the FileNet P8 system.

For the IBM Case Manager files and data, your backup plans can depend on how often files are used or changed.

For the additional components that you integrate with IBM Case Manager, see the product documentation to plan backup and recovery. For IBM Forms, back up both `ICM` and `API` directories within the IBM Forms installation path. For example, back up:

`C:\IBM\FormsServer\`*`installation path`*`\ICM`

`C:\IBM\FormsServer\`*`installation path`*`\API`

"Backing up FileNet P8 components" on page 69

"Backing up IBM Case Manager components" on page 69

Related information:

IBM FileNet P8 backup and recovery

Backing up FileNet P8 components

Periodically back up FileNet P8 components so that you can more rapidly recover from the loss of data.

About this task

Work with your backup administrator to prepare a plan for backing up the FileNet P8 data and assets that are associated with your IBM Case Manager system.

Determine the location of IBM FileNet P8 data in the FileNet P8 domain that is used by IBM Case Manager. This data set includes the global configuration database, object stores, workflow systems, and solutions. Also determine the location for all IBM Content Navigator data that is related to IBM Case Manager, including desktops and plug-ins.

See the following table for a list of FileNet P8 components to back up.

Table 4. FileNet P8 components and links to backup instructions

FileNet P8 components	Backup instructions
Global configuration database	Global configuration database backup
Object stores (design, staging, and target), workflow system, and file stores storage area	Object store backup
IBM Content Navigator	Backing up IBM Content Navigator
Optional: Case Analyzer	Case Analyzer store backup
Content Platform Engine server	Server configuration backup

Backing up IBM Case Manager components

Periodically back up IBM Case Manager components so that you can more rapidly recover from the loss of data.

About this task

Work with your backup administrator to prepare a plan for backing up IBM Case Manager components.

Procedure

To back up IBM Case Manager components:

- Back up the IBM Case Manager network share that hosts runtime plugins, Addons configuration, documents, and customized widget pages (run time). To determine the location of the directory to back up:
  1. In IBM Case Manager configuration tool, open your configuration profile.
  2. Right-click profile name and click **Edit Profile Properties**.
  3. Click **Next** twice, navigate to the Content Platform Engine definition page and locate the **Network shared directory** field.
- Back up the IBM Case Manager server.
  1. Back up all files and sub directories in `icm_installation_path\configure`.

2. Back up your application server profiles.

- Optional: Back up the IBM Case Manager rules repository directory. This backup step should be part of the Content Platform Engine file store backup policy. To determine the location of the directory to back up:
  1. In the IBM Case Manager configuration tool, open your configuration profile.
  2. Right-click **Configure Business Rules** in the profile pane and click **Edit Selected Task**. Locate Rules repository directory.
- Back up case management solutions (design time or run time) and customized widget pages (design time) by backing up the object store. See Object store backup.
- Optional: If you are using a case history store to record extended case history, determine the location of the case history store database. Include your plans for backing up the case history store as part of the backup of the IBM FileNet P8 domain.
  1. Determine the data source that was used for the case history database connection.
     - In the IBM Case Manager administration client, expand **Object Stores** in the Domain pane, then click the target object store.
     - Click **Case History Store** and note the value for the data source in the **Case history database connection** field.
  2. In your application server console, view the information for the data source. For example, in IBM WebSphere Application Server, the information is listed in the JDBC data sources. The database information is indicated in the Comment and required data source properties.

Restoring your system

You can restore your IBM Case Manager system by using your latest backups. Work with your backup administrator to understand the backup policy and the best way to perform the restore.

About this task

Start your restore with the IBM FileNet P8 components, then restore the IBM Case Manager components. To restore additional components that you integrate with IBM Case Manager, see the product documentation for recovery information. For IBM Forms, restore the `ICM` and `API` directories and restart the application server.

"Restoring FileNet P8 components"

"Restoring IBM Case Manager components" on page 71

Related information:

IBM FileNet P8 backup and recovery

Restoring FileNet P8 components

Start your restore with the foundation components in the IBM FileNet P8 domain. For each high-level step in your restore process, work with the backup administrator and use the appropriate product documentation to determine the specific steps that are required.

About this task

See the following table for a list of FileNet P8 components to restore.

Table 5. FileNet P8 components and links to recovery instructions

FileNet P8 components	Recovery instructions
Global configuration database	Recovering the data in your FileNet P8 domain
Object stores (design, staging, and target), workflow system, and file stores storage area	Recovering the data in your FileNet P8 domain
IBM Content Navigator	Refer to the backup information: Backing up IBM Content Navigator
Optional: Case Analyzer	Recovering the data in your FileNet P8 domain
Content Platform Engine server	Refer to the backup information: Server configuration backup

Restoring IBM Case Manager components

You can restore IBM Case Manager components by using your latest backups. Work with your backup administrator to understand the backup policy and the best way to perform the restore.

Procedure

To restore IBM Case Manager components:

- Restore IBM Case Manager servers.
  1. Reinstall the IBM Case Manager software as needed.
  2. Reconfigure the software or restore the IBM Case Manager configuration files from a backup.
- Restore the IBM Case Manager network share that hosts runtime plugins, Addons configuration, documents, and customized widget pages (run time) from the latest backup.
- Restore case management solutions (design time or run time) and customized widget pages (design time) by recovering the object store. See Recovering the data in your FileNet P8 domain.
- Optional: Restore the case history store database from the database server.
- Optional: Restore the business rules repository. Restore and overwrite the network shared directory from the latest backup.

Updating the Content Platform Engine client connector files

If your Content Platform Engine software has been updated since you configured IBM Case Manager, for example by installing a fix pack, you must update the corresponding client connector files on the IBM Case Manager server. After you install the updates, you must redeploy the IBM Case Manager application.

Before you begin

Check with the FileNet P8 Platform administrator to determine the update level of the Content Platform Engine. If no software updates have been applied, skip this task.

Procedure

To update the Content Platform Engine client connector files:

1. Start the configuration tool by running one of the following commands:

Operating system	Command
AIX	1. Change to the *_install_path*/configure directory. *_install_path* is the location where IBM Case Manager is installed, for example, /opt/IBM/CaseManagement. 2. Run the following command: `./configmgr`
Linux	1. Change to the *_install_path*/configure directory. *_install_path* is the location where IBM Case Manager is installed, for example, /opt/IBM/CaseManagement. 2. Run the following command: `./configmgr`
Linux for System z	1. Change to the *_install_path*/configure directory. *_install_path* is the location where IBM Case Manager is installed, for example, /opt/IBM/CaseManagement. 2. Run the following command: `./configmgr`
Windows	Perform one of the following actions: • Click **Start** > **All Programs** > **IBM Case Manager** > **Case Manager Configuration Tool**. • Run the following command: *_install_path*\configure\configmgr.exe *_install_path* is the location where IBM Case Manager is installed, for example, one of the following directories: – C:\Program Files\IBM\CaseManagement – C:\Program Files (x86)\IBM\CaseManagement

2. Open the profile that you created to configure the IBM Case Manager server for the environment that you are updating.
3. Run the Update the Content Platform Engine Client Connector Files task.
4. Restart the configuration tool.
5. Run the following IBM Case Manager configuration tool tasks:
   - Create Case Manager Applications
   - Deploy the Case Manager API
   - Deploy Workplace XT (optional, if you want the configuration tool to update, repackage, and redeploy Workplace XT)
   - Deploy Case Manager Builder Application

   For a production environment, skip the Deploy Case Manager Builder Application task.

Modifying an existing configuration

You can modify an existing configuration profile to change the profile property values or the property values of a task in the profile. For example, you can edit the task properties to correct errors that were found when you ran a task.

About this task

You can use the configuration tool to create a profile and edit a few properties in the profile and its tasks, and then save the profile without entering values for each of the properties. You can then open the profile later and edit the values to replace the default values or to change your previous values. If you did not run any of the tasks successfully yet, you can make unlimited modifications to the property values.

Editing some task values and running the task again on a working system can significantly affect your development environment or production environment. For example, if you change the name of the case management design object store after you create solutions, you lose access to your solution templates, to any existing connection definitions, and to related data in the previous design object store. To restore access, you must set the name of the case management design object store back to the original value.

Procedure

To modify an existing configuration profile:

1. If your configuration profile is not open in the configuration tool, open the profile:
   a. Click **File** > **Open Profile**.
   b. Enter the path to the profile or click **Browse** to locate the *profilename*`.cfgp` profile file. For example, select the `myDevelopment1.cfgp` file.
   c. Click **OK**.
2. Optional: If needed, edit the profile property values:
   a. Click **File** > **Edit Profile Properties**.
   b. Edit the existing property values.

      Tip: Click **Next** to view all properties.
   c. Click **Finish**. The properties are saved to the configuration XML file, but the property changes are not applied until you run the task that uses the properties.
3. Edit the property values for a specific task in the profile:
   a. Right-click the task name in the profile pane and select **Edit Task**.
   b. Edit the existing property values.
   c. Click **File** > **Save** to save your changes.
   d. Apply the property changes by right-clicking the task name in the profile pane and selecting **Run Task**. Running the configuration task can take several minutes. The task execution status messages are displayed in the console pane below the connection properties.

"Updating an object store" on page 74

"Synchronizing cases with solution data" on page 74

Updating an object store

You can update a design object store or target object store with IBM Case Manager releases. You can also update an object store to fix problems, such as to re-create any required IBM Case Manager folders that were accidentally deleted.

Procedure

To update an object store:

1. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   `http://server:port/navigator/?desktop=icmadmin`
   server is the IBM Content Navigator IP address or fully qualified server name.
   port is the IBM Content Navigator port number.
2. In the navigation tree in the left pane, select an object store.
3. On the object store page in the right pane, click **Actions** > **Update Object Store** and complete the wizard steps.

Synchronizing cases with solution data

Run the case synchronizer utility to update existing instances of a case type after you make changes to that case type.

By using the case synchronizer utility, you can update case instances to match changes that you make to the case type, such as:

- Adding new tasks
- Creating a new folder structure
- Updating the state of existing task instances in the case instances

The case synchronizer utility is in the IBM Case Manager installation folder.

Table 6. Case synchronizer file name and location

Platform	File name	Location
AIX	`caseSynchronizer.sh`	`/opt/IBM/CaseManagement`
Linux	`caseSynchronizer.sh`	`/opt/IBM/CaseManagement`
Linux for System z	`caseSynchronizer.sh`	`/opt/IBM/CaseManagement`
Windows	`caseSynchronizer.bat`	`C:\Program Files (x86)\IBM\CaseManagement`

Syntax

caseSynchronizer *command parameter-list*

parameter-list consists of a set of pairs, where each pair has a *parameter* and a *value*, separated by a space.

Commands

`launch`
Start the case synchronizer utility. The **launch** command requires parameters.

`suspend`
Stop the case synchronizer utility. The **suspend** command does not require parameters.

Parameters

-cews_uri
The web services URI to connect to Content Platform Engine, for example, http: //myserver:9080/wsi/FNCEWS40MTOM. This parameter is required.

-username
The user ID to connect to Content Platform Engine. This parameter is required.

-password
The password for the specified user ID to connect to Content Platform Engine. If the password is not specified, the case synchronizer utility will prompt for the password. This parameter is required.

-target_os
The target object store that the case synchronizer will check. This parameter is required

-caseType
The symbolic name of the case type for the tool to update. This parameter is required.

If the name of the case type includes spaces, surround the name with single quotation marks, for example, `-caseType 'Accident report'`.

-caseTypeFilter
The filter criteria to use when retrieving the case instances to update. This parameter is optional.

-includedTaskTypes
A comma-separated list of the task type symbolic names to add to the case instances. This parameter is optional.

-excludedTaskTypes
A comma-separated list of the task type symbolic names to exclude from the update to the case instances. This parameter is optional.

-file
The path to an input file that contains the parameters to run the tool. This parameter is optional.

If specified, the input file must include the **cews_uri**, **username**, **password**, **target_os**, and **caseType**parameters without leading hyphens.

-batchSize
The number of items to retrieve and process at one time. This parameter is optional. If not specified, the default batch size is 1000 items.

-threadPoolSize
The number of active threads for the tool to use when it processes case instances. This parameter is optional. The default value is 4.

For example, the following command starts the case synchronizer for cases of the type Accident Report and updates every case instance of that type with any changes that have been made to that case type.

```
caseSynchronizer launch -cews_uri http://myserver:9080/wsi/FNCEWS40MTOM
-username administrator -password mypassword
-target_os MyTargetOS -caseType 'Accident Report'
```

Customizing the case unique identifier prefix

After your solution is deployed, you can customize the case ID to a more user friendly value to display in the Case Manager Client by using IBM Administration Console for Content Platform Engine.

About this task

You can assign a case property as the Case Title Property, which is then used as the case title. Assign a property as the Case Title Property on the Views page of your solution in Case Manager Builder. Alternatively, you can customize the case unique identifier prefix after your solution is deployed.

By default, IBM Case Manager automatically assigns a unique case ID to a case type by using the case type unique identifier plus a 12-character number sequence. For example, a case type named Credit Application with a unique identifier of EXPL_CreditApplication might have a case identifier of EXPL_CreditApplication_00000010001.

Content Platform Engine supports a property on the deployed case type folder called Case Identifier Prefix. The Case Identifier Prefix property is an alphanumeric string up to six characters.

By changing the value of this property, the case prefix changes the automatically generated unique identifier to use this property value instead. For example, if you change the value of the Case Identifier Prefix to SAMPLE, the case unique identifier changes from EXPL_CreditApplication_00000010001 to SAMPLE_00000010001.

Tip: You can overwrite the entire case ID value that is displayed to the case worker in several ways. One way is to set the case ID value from a Content Platform Engine client application, such as the IBM Content Navigator browse feature, when you create a case folder using the application. Another way is to set the value of the Case Identifier (CmAcmCaseIdentifier) property on a Case Folder (CmAcmCaseFolder) object in a custom Content Platform Engine application.

Procedure

To customize the case unique identifier prefix:

1. In IBM Administration Console for Content Platform Engine, select the target object store to which the solution was deployed.
2. Browse to the case type folder by clicking **Browse** > **Root Folder** > **IBM Case Manager** > **Solution Deployments** > *Solution_Name* > **Case Types** > *Case_Type_Name*.
3. On the case type page in the right pane, click the **Properties** tab and modify the **Case Identifier Prefix** property to your new value.

Configuring your environment to show display names in Case Manager Client

You can configure your environment to support using the LDAP display name for users in widgets and search results in Case Manager Client.

About this task

The following widgets and dialogs can show a user's display name when the IBM Connections Profile plug-in is installed, and the option for showing the display name is enabled:

- In-basket widget
- Case List widget
- Document and History tabs in the Case Information widget
- Properties widget
- Timeline Visualizer widget
- Comment history in the Add Comment dialog box
- Custom Task Editor dialog box

Dialogs for reassigning users can also show user's display name.

Procedure

To enable the Case Manager Client to show display names:

1. Install the IBM Connections Profile plug-in in IBM Content Navigator:
   a. From the Administration View of IBM Content Navigator, click **Plugins** > **New Plug-in**.
   b. Specify the path of the plug-in JAR file in the IBM Content Navigator installation, for example, `/opt/IBM/ECMClient/plugins/ProfilePlugin.jar`.
   c. In the configuration section, select the **Show Display Name instead of Login Name** option.
   d. Click **Save** and **Close**.
   e. Log in to IBM Content Navigator as an administrator.
   f. Navigate to **Desktops** > **Case Manager** > **General**.
   g. In the **Plug-ins** area, select **Select the deployed plug-ins to enable for use with this desktop**. Then, select the IBM Connections Profile plug-in to be loaded for the IBM Case Manager desktop.
2. Configure the Content Platform Engine LDAP setting:
   a. Log in to IBM FileNet Enterprise Manager.
   b. Right click the root domain node.
   c. In the Properties panel, click the **Directory Configuration** tab and then click **Modify**.
   d. In the User tab, ensure that the **User Display Name Attribute** setting is set to **displayName** and that the displayName attribute in the LDAP server is populated with display name.

Customizing the case package PDF file

You can customize the appearance of the PDF file that is included in a case package. For example, you can change the fonts or include a company logo.

About this task

Case workers can create a case package to share details about a case with external stakeholders who do not have access to the case management system. For example, the case might need to be sent to a legal advisor for review. From the Case Details or Cases page, case workers can select properties, documents, related cases, and

other case information such as case comments and history, and package them into a single compressed file that is saved in the case folder. The case package contains the selected case documents and a PDF file that lists the selected case information.

You can customize the appearance of the PDF file by modifying the `casepackage.xsl` stylesheet file that is used by Apache FOP (Formatting Objects Processor) version 2.0 to generate the PDF file. For more information about customizing the stylesheet, see the Apache FOP documentation at https://xmlgraphics.apache.org/fop/.

Procedure

To customize the case package PDF file:

Modify the *network_shared_directory*`/AddOns/casePackage/casepackage.xsl` file in your development and production environments.

Important: Back up the customized stylesheet file before you install a patch or run the Register the IBM Case Manager Administration Client Plug-in configuration tool task. When you install a patch or run the Register the IBM Case Manager Administration Client Plug-in configuration tool task, the custimizations to the stylesheet are overridden.

Tuning IBM Case Manager

Reviewing the IBM Case Manager tuning information can help you improve and maintain the performance of IBM Case Manager.

Related concepts:

Performance tuning IBM FileNet P8 components

Adjusting the Java Virtual Machine (JVM) heap for IBM Case Manager

You can determine if the Java Virtual Machine (JVM) heap size is adversely affecting the performance of IBM Case Manager by monitoring the Java garbage collection history.

You can monitor the Java garbage collection history in one of two ways:

- You can enable verbose GC and review the resulting logs.
- You can run several JVM thread dumps and review the JVM activity during those times.

If the heap free space settles at 85% or more, consider decreasing the JVM minimum and maximum heap size values. However, do not set the JVM minimum and maximum heap sizes to the same value. Also, do not set the minimum heap

size value too high. Consider starting with a minimum heap size value of 256 MB. You can make additional adjustments as needed.

If physical memory is limited, ensure that the heap size values do not cause system paging activity. Although the IBM Case Manager server can be CPU intensive, it requires little I/O and should cause little to no system paging activity.

Tuning IBM Case Manager transmission protocols

Adjusting the following transmission protocols can improve IBM Case Manager performance.

IBM FileNet P8 Process Engine

If secured transmissions (such as FIPS) are not required, use the default IIOP protocol with IBM FileNet P8 Process Engine HTTP Tunneling increases both CPU usage and response time.

TCP/IP buffer size

Consider increasing the system TCP/IP buffer size from the default value. For example, on AIX use `no -o tcp_sendspace=524176` and `no -o tcp_recvspace=524176` to set the buffer size to 512 KB.

HTTP server

If an HTTP server is used as a load balancer for an application server cluster, increase the number of threads (or processes) accordingly for a high concurrency workload.

Tuning the IBM Case Manager object request broker (ORB)

Under moderate workloads, the default object request broker (ORB) settings work well.

Adjusting the following property values can improve performance during heavy workloads.

com.ibm.CORBA.ConnectionMultiplicity

Consider increasing the com.ibm.CORBA.ConnectionMultiplicity property value from its default setting of 1 to a value from 5 to 10.

com.ibm.CORBA.FragmentSize

Consider setting the com.ibm.CORBA.FragmentSize property value to 0. Increase this value as needed.

Web container thread pool

Monitor the web container thread pool and increase its size accordingly.

Indexing Content Platform Engine databases to improve IBM Case Manager performance

Depending on your solution and workload, you may find it beneficial to add indexes to some of the Content Platform Engine database to improve the

performance of IBM Case Manager. The following are some examples of these indexes, and the circumstances when they may be helpful.

i1 on container (creator, parent_container_id)
This index is for the advanced search on the Creator field. Create additional indexes depending on the fields that are used in the advanced search.

i2 on container (u<xy>_CMACMCASEIDENTIFIER,OBJECT__ID, object_class_id, home_id, ud956_cmacmcasestate, parent_container_id)
This index is for the basic search on the Case Identifier field. Create additional indexes depending on the fields used in the basic search.

i3 on event (u<xy>_CMACMCASEFOLDER, AUDIT_SEQUENCE desc)
This database retrieval index efficiently retrieves the case history in the Event table in target object stores. See Configuring production target object store indexes for details.

i4 on docversion (u<xy>_DOCUMENTTITLE)
Adding this index to avoid performance issues due to a table scan while searching documents under cases.

Setting the log size for Oracle case history databases

You might see a very high disk write queue length when using an Oracle database for case history. You can increase each `redo.log` file size to improve the disk write queue length.

Procedure

To increase the `redo.log` file size:

1. If the redo log group associated with the log file has a status of `CURRENT`, you need to first switch it with another group:
   ```
   alter system switch logfile;
   ```
2. Deactivate the redo log group you want to drop:
   ```
   alter system checkpoint;
   ```
3. Drop the redo log group from the database.
   ```
   alter database drop logfile group group_number
   ```

   Restriction: If you only have two redo log groups active on the Oracle database, you cannot drop the group, since Oracle databases require a minimum of two active redo log groups at all times. If this is the case, create a third temporary redo log group before dropping either of the other two groups. For example:
   ```
   alter database add logfile group 3 '/app01/oratest/oradata/BOTI/BOTI/redo03.log'
    size 100M;
   ```
4. Delete the `redo.log` file associated with the redo log group you just dropped.
5. Add the group back to the database with a larger specified size. For example, if you want to create the redo log group with a size of 100 MB:
   ```
   alter database add logfile group 2 '/app01/oratest/oradata/BOTI/BOTI/redo02.log'
    size 100M;
   ```

   Repeat for all other redo log groups, making sure to make them inactive before dropping them.
6. Activate the last redo log group that you added:
   ```
   alter system switch logfile;
   ```

Remember: If you originally had two redo log groups and you created a third temporary group to be able to drop the other two, you can delete this third group now.

Tuning the in-basket property synchronization settings

When a property value is updated in a case, the change is synchronized in all views of the case. You might experience performance issues if all property updates are set to synchronize automatically. To improve performance, you can disable the automatic synchronization for certain properties.

About this task

When you tune the property synchronization settings for performance reasons, choose properties that are not frequently updated.

At design time, you use Process Designer to save the event update settings as part of the solution. For solutions that are already deployed, you use Process Configuration Console to change the settings.

Procedure

To tune property synchronization settings:

1. From the Administration Console for Content Platform Engine, start the Process Configuration Console:
   a. Expand **Object Stores**.
   b. Expand your target object store.
   c. Select **Workflow System**.
   d. From the **Actions** menu, click **Configure Workflow Settings**.
2. Select the workflow isolated region that is associated with the solution that you are updating.
3. Right click the work queue that you are editing, and select **Queue Properties**.
4. On the Data Fields tab, clear the checkbox in the Event Update column for all properties that you want to disable synchronization for.
5. Commit your changes.

Tuning the maximum pool size for document rules

You may want to adjust the maximum pool size for document rules, depending on how many rules can be run in parallel by Content Platform Engine. You can tune the maximum pool size using the **-DrulesMaxPoolSize** parameter in the WebSphere Application Server profile for Content Platform Engine.

About this task

The default value for the **-DrulesMaxPoolSize** parameter is 100. The minimum value for the maximum pool size should not be less than the maximum number of rules that can be run in parallel in your system. For example, consider a system in which the Content Platform Engine has one target object store with two solutions with one casetype in each solution. Assume that only one rule can be run at a time in any case. In this situation, if you have 20 users that can be working with each solution, then there will be a maximum of 40 rules that can be run concurrently. In this example, the maximum pool size should not be set to a value smaller than 40. However, consider that when setting a value for the parameter that is too high

could result in an adverse memory impact on the Content Platform Engine Java Virtual Machine.

Procedure

To change the maximum pool size parameter value:

1. Add the following argument to the WebSphere Application Server profile for Content Platform Engine:

   ```
   -DrulesMaxPoolSize=NNN
   ```

   where `NNN` is the new value for the parameter.
2. Restart Content Platform Engine.

Security

You use security to configure access to the servers and applications that comprise your IBM Case Manager system. You also secure case objects and access when you configure security for a test or production-level solution.

Related concepts:

Planning for IBM Case Manager security

Planning for security

It is a best practice to keep security considerations in mind during all phases of the IBM Case Manager life cycle. Different administrators and business roles in your organization must collaborate to create effective and appropriate security for your IBM Case Manager environment and applications.

During the installation and configuration of IBM Case Manager, plan for administrator roles and access to the system. Before you create the case management object stores, it is a best practice to create a master group for users that you can assign at creation. This enables you to add users to the master group without changing the users on the object store.

For more information about planning users and groups for your development and production environments, see the following topics:

- Planning for security in the development environment
- Planning for security in the production environment

During solution design, create a plan for which case objects should be accessible to which case workers. When your solution is deployed, you can use the plan to configure appropriate security.

If the security requirements change for your solution, you can update the solution configuration and apply it to the solution.

Related information:

Planning for IBM Case Manager security

Configuring security for IBM Case Manager solutions

In both the development and the production environments, you configure security on the case management objects that are controlled by Content Platform Engine. You must also configure security on Content Platform Engine process services queues, rosters, and application spaces. For Case Manager Client, you configure view and edit access to pages.

About this task

You can assign permissions to different users, groups, and roles to determine the areas and objects of a solution in a FileNet P8 object store that these users can access. A set of permissions is called a security configuration.

Proper application of security can ensure that cases and case documents are visible and editable only by the appropriate users and groups. In the context of case management solutions, security involves several different types of objects:

- Case types
- Case folders and subfolders
- Documents
- Tasks
- Queues
- Rosters
- Comments
- Application spaces

The IBM Case Manager administration client provides a wizard that can help you to create, modify, delete, and apply a basic security configuration for your solution. The wizard provides a set of permissions that you can grant to the case worker groups that you created in your LDAP system. You use the IBM Case Manager administration client to set up a solution's security configuration and to transfer that security configuration from a user-acceptance testing environment or a staging environment into a production environment. The administration client simplifies the process of setting up security for objects, users, groups, and roles.

If your solution requires more complex permissions than the defaults that are provided by the wizard, you can also customize the permissions in the wizard. You can edit a privilege definition file that controls the permissions that are displayed and configured by the wizard. You can then use the updated wizard to create and apply a security configuration that contains these customized permissions.

Some environments have very specific or very rigorous security requirements. If the security requirements for your environment cannot be met by customizing the security wizard, you can also use the FileNet P8 security tools to set permissions manually on individual case objects.

"Configuring security by using the IBM Case Manager administration client wizard"

"Customizing privileges and permissions" on page 86

"Configuring security manually" on page 90

Configuring security by using the IBM Case Manager administration client wizard

In the production environment, you configure security on the case management objects that are controlled by Content Platform Engine. You must also configure security on Content Platform Engine process services queues, rosters, and application spaces. For Case Manager Client, you configure view and edit access to pages.

About this task

You can assign permissions to different users, groups, and roles to determine what areas and objects of a solution in a FileNet P8 object store that these users can access. A set of permissions is called a security configuration. You can use the IBM Case Manager administration client to create a security configuration for a solution. You can also transfer that security configuration from a user-acceptance

testing environment or a staging environment into a production environment. The administration client simplifies the process of setting up security for objects, users, groups, and roles.

To create or make changes to a security configuration by using the administration client, you must have administrator privileges. When you first create a security configuration, the administrators window in the security wizard is automatically populated with an entry, which is the current user who created the security configuration. This entry in the administrators window cannot be removed and is required to apply the configuration.

Attention: Add all users and groups that are required to administer solution deployment, security configuration, and audit configuration. Only the users and groups that you add as administrators with full control will be able to redeploy the solution, and reapply a security or audit configuration to the solution in the future.

Use the administration client in a test environment before you add those changes to a production environment. When you have applied and tested the security configuration in the test environment, migrate those changes to the production environment. Using the IBM Case Manager administration client in the test environment, export the security configuration. Then, in the production environment, use the IBM Case Manager administration client to import the security configuration.

Attention: Any changes that you make by using the administration client will overwrite existing security configurations.

The available settings in the wizard are the results of the solution design. The case types and roles that are displayed were created by the business analyst in Case Manager Builder during the design of the solution. Based on the security plan for the solution, you use the wizard to assign permissions for each type of case worker. For example, you might want the case worker role to have permission to view and update cases. You might grant another role, case auditor, permissions to view cases only.

When you apply a security configuration to a solution and the user is set in ICM_operations, case operations user permissions are applied to the solution as follows:

- **Case type class definition**: Read, Create instance, Read permissions (this object only)
- **Deployed case type folder**: Write (this object only). On this object and all children: View all properties, Modify all properties, File in folder/Annotate, Unfile from folder, Create subfolder, Delete, Read permissions, Modify permissions, Modify owner, Change state
- **Deployed solution folder**: Read (this object only)

Procedure

To configure security:

1. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   `http://server:port/navigator/?desktop=icmadmin`
   server is the IBM Content Navigator IP address or fully qualified server name.
   port is the IBM Content Navigator port number.

2. In the navigation tree in the left pane, select a design object store and click **Solutions**.
3. On the Solutions page in the right pane, select the solution for which to configure security.
4. Click **Actions** > **Manage** > **Security Configuration** and complete the wizard steps.

   Attention: To apply a security configuration to a solution, the solution must be deployed.

What to do next

If you want to further refine your security settings, you can use the same wizard to edit your existing configuration.

Related tasks:

"Exporting the security configuration" on page 134

"Importing the security configuration" on page 154

Customizing privileges and permissions

You can add, delete, or modify the permissions that you assign to roles and administrators in the IBM Case Manager administration client security configuration wizard.

About this task

By default, the "Modify permissions for roles" window in the security configuration wizard shows columns of predefined privileges that are available to assign to roles:

- create
- view
- update
- manage

Similarly, the "Define the administrators and assign privileges" window shows a single privilege by default: Full Control.

Each privilege consists of one or more permissions that are defined in a privilege definition file: `ICMPrivilegeDefinition.xml`. For example, the "create" default privilege consists of two permissions: createCase and startTask. The "create" privilege is defined in the privilege definition file as follows:

```
<secdef:privilegeDefinition name="create" category="icm">
     <secdef:allow>createCase</secdef:allow>
     <secdef:allow>startTask</secdef:allow>
</secdef:privilegeDefinition>
```

You can modify a privilege by adding or removing permissions in <secdef:allow> elements under each <secdef:privilegeDefinition> element. You can also remove a privilege column from the security configuration wizard by removing the corresponding <secdef:privilegeDefinition> element and its associated <secdef:allow> child elements.

For example, if your organization does not require a "manage" privilege to assign to roles, you can remove this privilege from the security configuration wizard by removing the following lines from the privilege definition file:

```
<secdef:privilegeDefinition name="manage" category="icm">
     <secdef:allow>manageCase</secdef:allow>
     <secdef:allow>startTask</secdef:allow>
     <secdef:allow>manageRole</secdef:allow>
</secdef:privilegeDefinition>
```

You can add a new privilege to the security configuration wizard by adding a new <secdef:privilegeDefinition> element with appropriate <secdef:allow> child elements. In the <secdef:privilegeDefinition> element, specify category="icm" to add the privilege to the "Modify permissions for roles" window in the security configuration wizard. Specify category="admin" to add the privilege to the "Define the administrators and assign privileges" window.

For example, you can add a new "view and comment" privilege that consists of viewCase and addComment permissions. This privilege might be useful if you have an auditor role to which you want to assign viewing and commenting permissions. Add the "view and comment" privilege to the security configuration wizard by adding the following lines to the privilege definition file:

```
<secdef:privilegeDefinition name="view and comment" category="icm">
     <secdef:allow>viewCase</secdef:allow>
     <secdef:allow>addComment</secdef:allow>
</secdef:privilegeDefinition>
```

After you edit the security privilege definition file and check it in, your changes are reflected in the administration client security configuration wizard. For example, in the previous example, a column entitled "Custom Permission: view and comment" is added to "Modify permissions for roles" window in the security configuration wizard.

Procedure

To customize privileges:

1. Using IBM FileNet Enterprise Manager, navigate to the `ICMPrivilegeDefinition.xml` file in the *`object_store_name`*`\Root Folder\IBM Case Manager\Security Configurations\Privilege Definitions` folder and check out the file.
2. Add, modify, or delete privileges by editing the `ICMPrivilegeDefinition.xml` file. See the comments in the file for descriptions of all available permissions.
3. Check in the revised `ICMPrivilegeDefinition.xml` file by using IBM FileNet Enterprise Manager. In the Check In Content window, ensure that the **Automatically classify this document version on Check In** option is selected.
4. Run the security configuration wizard in the IBM Case Manager administration client to view your changes.

"Privilege definition reference"

Privilege definition reference

The security configuration wizard in the IBM Case Manager administration client sets permissions on workflow and content objects. A set of predefined privileges are available in the security configuration wizard by default. You can customize the default settings by editing the privilege definition file.

Table 7. Default privileges in the security configuration wizard

Privilege	Allows	Sets	Applies to	What is updated?
create	createCase	"view all properties" "create instance" "read permissions"	"this object only"	Case Type Subclass: TOS > Other Classes > Folder > Base Case > Case Folder > CaseType
		"modify all properties"	"this object only"	Deployed Case Type Folder
		"view all properties" "create subfolder" "file in folder/ annotate" "read permissions"	"this object and all children"	Deployed Case Type Folder
	startTask	"change state"	"this object and all children"	Deployed Case Type Folder
		"create"		Process region roster
view	viewCase	"view all properties" "read permissions"	"this object and all children"	Deployed Case Type Folder

Table 7. Default privileges in the security configuration wizard (continued)

Privilege	Allows	Sets	Applies to	What is updated?
update	viewCase	"view all properties" "read permissions"	"this object and all children"	Deployed Case Type Folder
	updateCase	"modify all properties"	"this object and all children"	Deployed Case Type Folder
	addDocument	"file in folder/ annotate" "unfile from folder"	"this object and all children"	Deployed Case Type Folder
	createSubfolder	"create subfolder"	"this object and all children"	Deployed Case Type Folder
	addComment	"file in folder/ annotate"	"this object and all children"	Deployed Case Type Folder
	createDiscretionary Task	"view all properties" "create instance" "read permissions"	"this object only"	Discretionary task type subclass: TOS > OtherClasses > Task > CaseTask > MyDiscretionaryTask
	createDynamicTask	"view all properties" "create instance" "read permissions"	"this object only"	Discretionary task type subclass: TOS > OtherClasses > Task > CaseTask > MyDynamicTask
	startTask	"change state"	"this object and all children"	Deployed Case Type Folder
		"create"		Process region roster
	viewWork	"query"		Process region role: Process Configuration Console > Work Queues > SolPrefix_Role > Security Tab
	processWork	"process"		Process region role: Process Configuration Console > Work Queues > SolPrefix_Role > Security Tab

Table 7. Default privileges in the security configuration wizard (continued)

Privilege	Allows	Sets	Applies to	What is updated?
manage	manageCase	"view all properties" "modify all properties" "file in folder/ annotate" "unfile from folder" "create subfolder" "delete" "read permissions" "modify permissions" "modify owner" "change state"	"this object and all children"	Deployed Case Type Folder
	startTask	"change state"	"this object and all children"	Deployed Case Type Folder
		"create"		Process region roster
	manageRole	"write"		Process Configuration Console > Application Space > Solution > Security
full control	FullControl		"this object and all children"	Deployed Solution Folder
			"this object only"	TOS/OtherClasses/Task/CaseTask/ MyDiscretionaryTask TOS > Other Classes > Folder > Base Case > Case Folder > CaseType

Configuring security manually

The administration client security wizard provides basic case security. However, if you want to use a different security model or more specific settings, you can edit the permission settings on the case objects that are controlled by Content Platform Engine. You can also manually configure security for process services.

About this task

Your environment might have different security requirements than the model that is provided by the security wizard. In addition, your customized security scheme might require additional security configuration steps. Work with your solution and security administrators to ensure that appropriate security settings are applied to meet your business requirements.

Configuring security in Content Platform Engine

You can use IBM Administration Console for Content Platform Engine to edit the permission settings on the case objects that are controlled by Content Platform Engine.

Permissions for IBM Case Manager objects:

Each Content Platform Engine object such as a folder or document has an Access Control List (ACL) containing the permissions for the object. An ACL is a collection of Access Control Entries (ACEs), where each ACE grants or denies a set of permissions to a user or group.

For some objects, you can set permissions directly on the target object. This permission type is called direct ACEs. Some objects inherit permissions from another Content Platform Engine object. This permission type is called inherited ACEs.

The following Content Platform Engine classes are relevant to IBM Case Manager:

- Case folders
- Case subfolders
- Tasks
- Case comments
- Documents

Direct ACEs

When an object is created, the creating application can specify its own set of direct ACEs. Other direct ACEs are copied from the Default Instance Permissions of the object ClassDefinition.

For IBM Case Manager cases and most of their related objects, it is a best practice to configure permissions through inheritance from the Case Type folder, rather than through the Default Instance Permissions of the Case Type class. Even if you configure permissions through inheritance, Default Instance Permissions can still apply to cases and case-related objects that are created. The default permissions are not always correct for these objects. You can edit these settings directly as required.

Inherited ACEs

Because the IBM Case Manager event handlers enforce that case folders reside underneath the Case Type folder, these folders should inherit their permissions

from this case folder. This inheritance allows permissions for all cases of a given type to be easily adjusted by changing the permissions on the case type folder.

To make security configuration of other case-related objects more manageable, all of the other case-related objects should inherit permissions from the case object that they are associated with. This security inheritance is configured by using security proxy properties on case subfolders, tasks, and case comments, as follows:

Case subfolders
Inherit security from the case folder through the system defined security proxy property Folder.Parent.

Case comments
Inherit security from the case folder through the system-defined security proxy property Annotation.AnnotatedObject. Case comments are annotations on the case folder.

Tasks Inherit security from the case folder through the system defined security proxy property Task.Coordinator.

CreateInstance permission

Access for creating an instance of a class is controlled by granting the CREATE_INSTANCE permission on the ClassDefinition for the class. This access is granted in the class permissions, not the Default Instance Permissions. By default, CREATE_INSTANCE permission is granted to #AUTHENTICATED_USERS, which means anyone who can log in to the Content Platform Engine. For content management solutions, this setting means that anyone who can log in can create a document. For case management solutions, however, this permission might not be appropriate. You might want to allow only certain groups to create a case, task, case comment, or document.

Document classes

While documents can be associated with a case, they can also be used outside of the case at the same time. Because of this variation, the case cannot influence the document permissions. System administrators must configure default permissions by using default instance security for case-associated Document classes the same as for documents that are not associated with a case.

Setting permissions for the solution folder:

In the Security settings for the solution folder, you can specify which users have rights to the solution folder. Only users who have permission to view the solution folder can work with the solution in Case Manager Client.

Procedure

To set permissions on the solution folder:

1. To find the solution folder, navigate to the following path within the object store in IBM Administration Console for Content Platform Engine: **Browse** > **Root Folder** > **IBM Case Manager** > **Solution Deployments** > ***Solution name***.
2. Click the **Security** tab and click **Add** to add users or groups to the list. If a user or group no longer requires permissions on the solution folder, select the user or group and click **Remove**.

3. For regular users or groups, specify the View properties permission level and apply to this object only. For administrators, specify the Full Control permission level and apply to this object and all children.

Setting permissions for a case type class:

In the Security settings for a case type class, you can specify which users have permission to create a case. You can also specify which creators can retain control over the case.

About this task

The default setting for CREATE_INSTANCE allows any user who can log in to create a case. If you want to allow only certain users to create cases, this default setting is not appropriate. You can change the permissions on the case type class.

The default setting of #CREATOR-OWNER allows the creator of a case to retain full control over the case and remain the owner of record. If you do not want the creator of a case to retain full control over the case, then the default value for owner is not appropriate. You can change the setting to make the owner value blank, or you can assign ownership to a group.

Procedure

1. To find the case type class in IBM Administration Console for Content Platform Engine, navigate to a deployed solution within an object store. Case type classes for an object store are found in the following Administration Console for Content Platform Engine path: ***Object store name*** > **Data Design** > **Classes** > **Folder** > **Base Case** > **Case Folder**.
2. Click the desired case type class in the list and change the CREATE_INSTANCE permission:
   a. Click the **Security** tab and in the **Name** list, select #AUTHENTICATED_USERS and click the **Edit...** button.
   b. Clear the **Create instance** check box and make any other changes as desired.
   c. Click **Add** to add one or more groups to the list.
   d. Click the appropriate check boxes to add the required permissions, such as **Create instance**.
   e. Save your changes.
3. Change the #CREATOR_OWNER setting to blank, or assign ownership to a specific group:

Option	Description
Set the owner value to blank	1. On the Default Instance Security tab, click **Change Owner**. 2. Click the **Set Default Owner to NULL** radio button. 3. Save your changes.

Option	Description
Assign ownership to a group	1. On the Default Instance Security tab, click **Change Owner**. 2. Click the **Change default owner to:** radio button and click the **Find** button. Search for and then add the name of a group (such as Case administrators) by moving the group from the Available Users and Groups list to the Selected Users and Groups list. 3. Click OK to save your changes.

Setting permissions for a case type folder:

You use the Security settings in the Properties dialog to configure permissions for specific groups. You can add the groups and specify general permission levels and custom settings.

Procedure

To set permissions on the case type folder:

1. To find the case type folder, navigate to the following path within the object store in IBM Administration Console for Content Platform Engine: **Browse** > **Root Folder** > **IBM Case Manager** > **Solution Deployments** > ***Solution name*** > **Case Types** > ***Case type name***.
2. Click the **Security** tab and click **Add...** to add one or more groups to the list.
3. For each group, specify the appropriate permission level.

   Important: For each entry, set the **Apply To:** drop-down setting to **This object and all children**. This setting ensures that the permissions are inherited by all objects that have established a security proxy relationship to the case.
   For the sample groups, grant the following permissions:

Table 8. Sample groups and permissions

Group	Permissions
Case Administrators	Full Control
Case Initiators	View Properties, plus Modify Properties, Create subfolder and File in folder/Annotate rights, Read Permission rights
Case Workers	Modify
Case Viewers	View Properties
#AUTHENTICATED_USERS	No access. Delete this entry in the permissions list.

Setting permissions for discretionary task classes:

For discretionary task class permissions, you can specify whether all logged-in users can create discretionary tasks. You can also specify whether users who create discretionary tasks can also have permission to modify those tasks.

About this task

The default setting for CREATE_INSTANCE allows any user to create a discretionary task. If you want to allow only certain users to create discretionary tasks, this default setting is not appropriate. You can change the permissions on the discretionary task class.

Tasks are created by the Content Platform Engine server when a case is created. Tasks inherit permissions from the case that owns them. User-created, or discretionary tasks, are created by users. It is a best practice to set user-added discretionary task class permissions to ensure that the #CREATOR-OWNER user who created the discretionary task class can change the state or modify the properties.

Procedure

To set permissions on discretionary task classes:

1. Navigate to your discretionary task class in the following path in Administration Console for Content Platform Engine: **Data Design** > **Classes** > **Other Classes** > **Task** > **Case Task** > ***Name based on case type***.
2. Click the desired discretionary task class in the list.
3. Click the **Security** tab, and in the **Name** list, select #AUTHENTICATED_USERS and click the **Edit** button.
4. Clear the **Create instance** check box and make any other desired changes to permissions. Click **OK**.
5. Click **Add** to add one or more groups to the list.
6. Add the required permissions, including **Create instance** if appropriate, by selecting the check boxes. Click **OK**.
7. Click the **Default Instance Security** tab and select **#CREATOR-OWNER**.
8. Click **Edit**. Select the **Modify all properties** check box.
9. Click **OK**. Under Default Instance Owner, click **Change Owner**.
10. Under **Change default owner**, find and select `#CREATOR_OWNER` and click **OK**.

Setting permissions for custom task classes:

For custom task class permissions, you can specify whether all logged-in users can create tasks. You can also specify whether users who create custom tasks can also have permission to modify those tasks.

About this task

The default setting for CREATE_INSTANCE allows any user to create a custom task. If you want to allow only certain users to create custom tasks, this default setting is not appropriate. You can change the permissions on the custom task class.

Custom tasks are created by users. When a custom task is created, it inherits the security from the case to which it belongs. It is a best practice to set user-added task class permissions to ensure that the #CREATOR-OWNER user who created the task class can change the state or modify the properties.

Procedure

To set permissions on custom task classes:

1. Navigate to your custom task class in the following path in Administration Console for Content Platform Engine: **Data Design** > **Classes** > **Other Classes** > **Task** > **Case Task** > **Dynamic Task**.
2. Click the desired custom task class in the list.
3. Click the **Security** tab, and in the **Name** list, select #AUTHENTICATED_USERS or the master group and click the **Edit** button.
4. Clear the **Create instance** check box and make any other changes to permissions. Click **OK**.
5. Click **Add** to add one or more groups to the list.
6. Add the required permissions, including **Create instance** if appropriate, by selecting the check boxes. Click **OK**.

Setting permissions for case comments:

The permission to create a case comment is granted by default to #AUTHENTICATED_USERS, meaning that anyone who can log in and has `File in Folder / Annotate` permissions on the case type instance can create a case comment. You can change this setting to match the requirements of your environment.

About this task

The default setting for CREATE_INSTANCE allows any user who can log in to create a case comment. If you want to allow only certain users to create case comments, this default setting is not appropriate. You can change the permissions on the case comment class.

Procedure

To change the CREATE_INSTANCE permission:

1. Navigate to the Case Comment class (or comment subclass, if appropriate) in the following path in Administration Console for Content Platform Engine: **Data Design** > **Classes** > **Other Classes** > **Annotation** > **Case Comment**.
2. Click the **Security** tab for **Case Comment** and in the list, select #AUTHENTICATED_USERS.
3. Click the **Edit...** button, and clear the **Create instance** check box. Make changes to any other desired permissions and click **OK**.
4. Click the **Add...** button to add one or more groups to the list.
5. Add the required permissions, including **Create instance** if appropriate, and click **OK**.

What to do next

For each entry, set the **Apply To:** setting to **This object and all children**. This setting ensures that the permissions are inherited by the child classes of Case Comment class.

Setting permissions for case relationships:

The permission to create a case relationship is granted by default to #AUTHENTICATED_USERS, meaning that anyone who can log in can create a case relationship. To create a relationship between two cases, a user must have

view rights on both cases. The permission to delete a case relationship is granted by default only to the administrator. You can change these settings to match the requirements of your environment.

About this task

The default setting for CREATE_INSTANCE allows any user who can log in to create a case relationship between two cases that the user has view rights with. Also, the default setting for DELETE allows only an administrator to delete a case relationship. If you want to allow only certain users to create or delete case relationships, the default settings might not be appropriate. You can change the permissions on the case relationship class.

Procedure

To change the case relationship class permission:

1. Navigate to the Case Relationship class in the following path in Administration Console for Content Platform Engine: **Data Design** > **Classes** > **Other Classes** > **Link** > **Case Relationship**.
2. Click the **Case Relationship** class and click the **Security** tab.
3. Change the CREATE_INSTANCE permissions:
   a. In the list, select #AUTHENTICATED_USERS and click the **Edit...** button.
   b. Clear the **Create instance** check box, and make any other desired permissions changes, and click **OK**.
   c. Click the **Add...** button to add one or more groups to the list.
   d. Add any required permissions, including **Create instance** if appropriate, and click **OK**.
4. Change the DELETE permissions:
   a. In the list, select #AUTHENTICATED_USERS and click the **Edit...** button. Check the **Delete** check box to allow all users to be able to delete case relationships, and make any other desired permissions changes, and click **OK**.
   b. Or, click **Add** to add one or more groups to the list. Add the required permissions, including **Delete** if appropriate, and click **OK**.

Configuring security in Content Platform Engine process services

For Content Platform Engine process services, you configure security for queues of work items and specify which users are permitted to launch workflows. You can also configure permissions for certain users to change role assignments.

"Content Platform Engine process services groups"

"Configuring queues to allow users to process work items" on page 98

"Configuring the roster to enable launching task workflows" on page 101

"Configuring the application space to enable setting role membership" on page 103

Content Platform Engine process services groups:

You assign Content Platform Engine process services access rights to two main groups, the workflow system administration group and the workflow system configuration group. You use these groups to specify what process actions are available to users of your case management solution.

The following two groups have special access rights in the Content Platform Engine. During the configuration of the FileNet P8 Platform, these groups are assigned to a Lightweight Directory Access Protocol (LDAP) group name.

Table 9. Content Platform Engine groups

Group	Description
Workflow system administration group	Required. Users in this group have full rights to all workflow rosters and queues, and can unlock work items locked by other users.
Workflow system configuration group	Recommended. If this group is assigned to an LDAP group, only users who belong to this group or the workflow system administration group can modify system configuration through the Process Configuration Console or through APIs.

If the workflow system configuration group is not configured, system administration group members and all users can manage roles. If the workflow system configuration group is configured, only the following users can manage roles:

- workflow system configuration group members
- users and groups with write permissions to the application space

The following table summarizes how solution assets map to securable entities in the Content Platform Engine.

Table 10. Case management to Content Platform Engine mapping

Content Platform Engine entity	Case management solution component
Queue	One queue per role in a solution
Roster	One roster per solution
Application space	One application space per solution

Event log data is included in the case history, which uses the same security as is applied to case instances.

If you do not assign anyone to an access right for a roster or queue, then everyone has that right. For example, if you do not assign anyone to the Query access right on the roster, then all users can Query. As soon as you assign at least one user or group to have Query rights, then only those users and the P8 Admin role can Query.

You must assign rights on the application space in order to modify role membership. If you do not assign any rights, then only the workflow system administration group and the workflow system configuration group can modify role membership.

Members of the workflow system administration group have full rights to everything, even if you do not explicitly assign rights to this group.

Configuring queues to allow users to process work items:

Queues hold work items waiting to be processed. You can grant users access to query and process the work items in a particular queue.

Procedure

To configure queue permissions:

1. In Administration Console for Content Platform Engine, select the object store to which the solution was deployed, and click **Administrative** > **Workflow System**.
2. On the Workflow System tab, click **Actions** > **Configure Workflow Settings**.
3. From the **Workflow Systems** list, select the connection point for the project area where the solution application resides. In the **Action** menu, click **Connect** to log on to the workflow system.
4. Navigate to the work queue in the left pane, and highlight the work queue you want to configure.
5. Right click the work queue and click **Properties**.
6. Click the Security tab, and select **Groups**.
7. Select the group for which you want to assign permissions, and move the group to the Selected Users window.
8. Set the Default rights, and click **OK**.

Example

For the example runtime user groups, you might assign the following permissions for each role:

Table 11. Queue permissions by group

Group	Permissions
Case viewers	None. In most situations, a member of the case viewer user group does not need to view work items, but instead might search for and view cases. Therefore, those users will have the right to view only the case objects in Content Platform Engine. If a member of the case viewer user group needs to see work items in a queue without opening or processing them, then those users must have Query permissions. If a user with only Query permission tries to open a work item, an error occurs.
Case initiators	Query and Process, but only if case creators must also view and process work items.

Table 11. Queue permissions by group (continued)

Group	Permissions
Case workers	Query and Process Each role is associated with an LDAP group or groups. Any users who must process work items in that role must be in a group given Query and Create rights to the role queue. For example: • Users in the Clerks role are added to the Clerks group. The Clerks group is given Query and Process rights to the Clerks queue. • Users in the Supervisors role are added to the Supervisors group, which is given Query and Process rights to the Clerks queue.
Case administrators	Query and Process A case administrator requires Query rights, but might also require Process rights if they must troubleshoot work items.

"Queue permissions"

Queue permissions:

Queue permissions determine what actions a user can take on a queue. Typically, case workers need both Query and Process permissions on the role Queue.

For each role in a solution, one work queue is created. In addition to work queues, there is an Inbox queue which holds work items assigned to users. Case Manager Client users see in-baskets that represent a view into the queue. In-baskets do not need an additional security setting, as only the queues behind the in-baskets are configured for security.

Queues permit the following access rights:

Table 12. Queue access rights

Permission	Access rights
Query	View work items. If no user or group is assigned, any user can view items in the queue.

Table 12. Queue access rights (continued)

Permission	Access rights
Process	Lock, modify, save, and complete work items. If no user or group is assigned, any user can process items in the queue. Process permission applies to the queue in which the work item is locked, rather than to the destination queue. The destination queue is the queue to which the work item is dispatched upon completion of the step. The destination queue is under system control, not user control.

In addition to case workers, any user who must assign or reassign work must also be given Query and Process rights.

The Inbox queue does not usually need extra security because all users access the queue, but the system will filter and return only the work items for the current user automatically. You can also limit access to the Inbox queue to only case workers who process work items for the solution.

Configuring the roster to enable launching task workflows:

You use a roster to control which users can launch a workflow. Most case workers need Create permission on the roster. Roster permissions are assigned in the Process Configuration Console.

Procedure

To configure the roster:

1. In Administration Console for Content Platform Engine, select the object store to which the solution was deployed, and click **Administrative** > **Workflow System**.
2. On the Workflow System tab, click **Actions** > **Configure Workflow Settings**.
3. Navigate to the rosters in the left pane, and highlight the roster that you want to configure.
4. Right click the roster and click **Properties**.
5. Click the Security tab, and select **Groups**. Select the group for which you want to assign permissions, and move the group to the Selected Users window.
6. Set the Default rights, and click **OK**.

Example

For the example runtime user groups, you might assign the following permissions on the roster:

Table 13. Queue permissions by group

Group	Permissions
Case viewers	None.

Table 13. Queue permissions by group (continued)

Group	Permissions
Case initiators	Create. When the case is created, workflows associated with tasks are launched on behalf of the user who created the case.
Case workers	Create. If case workers must create new tasks or start tasks, they must have Create rights on the roster in order to launch the workflow. Because there is only one roster for the entire solution, you should specify all groups that are associated with roles to have Create rights on the roster.
Case administrators	Query and Create A case administrator needs Query rights for troubleshooting. If administrators must start tasks, grant administrators Create rights as well.

Important: If you are using IBM Content Manager as your document repository with IBM Case Manager, you must also grant the *cm8intid* user **Create rights** privileges to the rosters of your solutions.

"Roster permissions"

Roster permissions:

A workflow roster is a database structure that stores information about all workflows in an isolated region. Workflow rosters provide Content Platform Engine workflow administrators an efficient way to locate specific active workflows.

Rosters permit the following access rights:

Table 14. Roster access rights

Permission	Access rights
Query	View the roster summary of the work item. Users can also view the work item itself if they have read access to the queue containing the work item. If no user or group is assigned, any user can query the roster.
Create	Launch a workflow. If no user or group is assigned, any user can launch a workflow.

In a case management solution, case workers must be given Create rights on the roster associated with the solution. These rights ensure that workflows that are associated with tasks are launched when the worker performs the action on the case. Tasks can move to the Working state, causing workflows to launch, in several ways:

- A new case is created. Any automatic tasks that have no preconditions, or where the preconditions are already met, are launched when the case is created. The user who created the task must have Create rights on the roster.
- A document is created and added to the case. If there is a precondition that causes a task to move to the Working state because a document is added to the case, the user who adds the document must have Create rights on the roster.
- A case property is updated. If there is a precondition that causes a task to move to the Working state because of a property value update, the user who updates the property must have Create rights on the roster.
- A manual task is started. When the user manually starts a task, the workflow is launched. The user who starts the task must have Create rights on the roster.
- A new task is created. Any user who creates new user-defined or discretionary tasks must have Create rights on the roster.

Configuring the application space to enable setting role membership:

You use the application space to manage roles in the Content Platform Engine. Every role belongs to an application space. A case management solution has one application space.

About this task

When a user logs in to a solution, they are shown the roles that they can act in. They can only select a role in which they are currently a member. You can set only one access right for the application space, the right to modify the users and groups assigned to all roles in that application space. For case management, any users who make role assignments must be given rights to the application space. It is a best practice to assign an LDAP group or groups to the application space to control who can manage roles. This group can be the same as one of your LDAP groups that map to a role, for example, Supervisors.

Procedure

To configure the application space to enable setting role membership:

1. In Administration Console for Content Platform Engine, select the object store to which the solution was deployed, and click **Administrative** > **Workflow System**.
2. On the Workflow System tab, click **Actions** > **Configure Workflow Settings**.
3. Navigate to the Application Spaces in the left pane, and highlight the application space that you want to configure.
4. Right click the application space and click **Properties**.
5. On the **Security** tab, select **Groups**.
6. Select the group for which you want to assign permissions, and move the group to the Selected Users window.
7. Click **OK**.

   Important:
   Defining role membership does not give users the rights to process work items in a queue. You must set up the rights on the queue separately. When setting up your groups, make sure that all case workers who might be assigned to a role have been granted Process rights on the role queue.

Changing role assignments in the application space

A supervisor who has the rights to change role assignments can adjust the membership of a role when there is a large backlog of work to complete.

In this example, there are two groups:

- Legal Reviewers: Bob, Srini, Gai
- Legal Reviewers Backup: Sally

The queue for these tasks is called Legal Reviewers. In this queue, the Legal Reviewers group and the Legal Reviewers Backup group have Query and Process Rights.

Normally, only the Legal Reviewers group is assigned to the Legal Reviewers role. However, during times of heavy workload, the supervisor can add the Legal Reviewers Backup group to this role. Sally can then help with the Legal Review tasks when needed.

Configuring single sign on security

IBM Case Manager supports the configuration of single sign on (SSO) by using Tivoli Access Manager for e-business, CA eTrust SiteMinder, or Kerbero Spnego.

"Configuring IBM Case Manager to support SSO through IBM Tivoli Access Manager for e-business"

"IBM Case Manager and form-based authentication for Single Sign-On (SSO)" on page 105

"Configuring IBM Case Manager to support SSO through CA eTrust SiteMinder" on page 106

"Configuring IBM Case Manager to support SSO through Kerberos SPNEGO" on page 108

"Configuring IBM Case Manager to support SSO through IBM Security Access Manager for Web" on page 110

"Configuring IBM Case Manager to support SSO through SAML" on page 111

"Verifying your SSO deployment" on page 113

Configuring IBM Case Manager to support SSO through IBM Tivoli Access Manager for e-business

You can configure IBM Case Manager to support single sign-on (SSO) authentication through IBM Tivoli Access Manager for e-business.

Before you begin

Before you configure SSO support, you must complete these tasks:

1. Install, configure, and verify the deployment of your IBM Content Navigator environment with Tivoli Access Manager for e-business by completing the predeployment tasks.
2. Install, configure, and verify the deployment of IBM Case Manager.

About this task

You might need to modify the following steps according to your system environment. Consult your system administrators for modifications that are specific for your environment.

Procedure

To configure SSO support for IBM Case Manager by using Tivoli Access Manager for e-business:

1. Configure the permissions for IBM Case Manager users. IBM Case Manager users require permissions for the PUT and POST methods, which are not allowed by the default ACL of the Webseal instance.
   a. Log in to the Tivoli Access Manager for e-business web console and navigate to **Tivoli Access Manger** > **Web Portal Manager** > **Object Space** > **Browse Object Space**.
   b. Expand the object tree to locate the default access list for Webseal, `default-webseal`.
   c. Under Groups, click **Create Group**, and create a group named `icm-users`. Add your IBM Case Manager users such as administrator, testid, and any others, to the `icm-users` group.
   d. Add the permissions for the IBM Case Manager users. Open the `default-webseal` access list and click **Create** to create an ACL entry. Check all required permissions for the entry type group and the `icm-users` group.
2. Create junctions to the IBM Case Manager IBM HTTP Server. Start the **pdamin** utility and create transparent junctions for all the paths for IBM Case Manager. At a minimum, create junctions for all of the following paths:
   - `CaseForms/`
   - `CaseBuilder/`
   - `CaseManagerHelp/`
   - `CaseManager/`
   - `ICMClient/`

   For example, the following **pdadmin** command creates the junction to IBM Case Manager:

```
pdadmin sec_master server task wd1-webseald-iam.iamdemo.tivoli.com
  create -t ss l -f -b supply -c iv_creds -x -h 9.119.90.107
  -p 9447 /CaseManager
```

What to do next

For information about handling the `favicon.ico` file with Mozilla Firefox, see Handling the favicon.ico file with Mozilla Firefox.

Related tasks:

"Verifying your SSO deployment" on page 113

IBM Case Manager and form-based authentication for Single Sign-On (SSO)

The IBM Case Manager configuration tool does not support the **Application server form-based authentication** option in the IBM Content Navigator configuration profile. This problem can prevent users from running certain tasks.

The **Application server form-based authentication** option is specified for **IBM Content Navigator authentication** in the **Configure the IBM Content Navigator Web Application** step of the IBM Content Navigator configuration profile. This configuration profile is run in the IBM Content Navigator Configuration and Deployment tool ("`\ECMClient\configure\configmgr.exe`").

If SSO is configured with the **Application server form-based authentication** option, users who run certain tasks in the IBM Case Manager configuration tool can receive the `java.io.IOException: stream is closed` error. Alternatively, the users might receive a similar error message that relates to network connectivity or configuration.

The IBM Case Manager configuration tool does support SSO for IBM Content Navigator. The following table describes the IBM Case Manager configuration tool for each of the three **IBM Content Navigator authentication** options:

Table 15. IBM Content Navigator authentication options

IBM Content Navigator authentication	IBM Case Manager configuration tool
IBM Content Navigator desktop authentication	This option is always supported. It does not work with SSO but can be used as a temporary workaround for running the IBM Case Manager configuration tool while SSO is disabled.
Application server authentication	This option is supported even if a form is used by the SSO server, if the form used is either the default form for the SSO provider or, if it is a custom form, that it implements the same fields (in the same sequence) and the same authentication logic as the default form for the SSO provider. If the SSO provider used is IBM Tivoli Access Manager for e-business, you must also configure basic authentication as a fallback. To configure basic authentication in this way, set `"ba-auth = both"` in the WebSEAL configuration file. Failure to set this value prevents the IBM Case Manager configuration tool from connecting to the IBM Content Navigator deployment in the associated application server.
Application server form-based authentication	This option is not supported by the IBM Case Manager configuration tool.

Other configurations or expedients might work, but are not officially supported.

Configuring IBM Case Manager to support SSO through CA eTrust SiteMinder

You can configure IBM Case Manager to support single sign-on (SSO) authentication through CA eTrust SiteMinder.

Before you begin

Before you configure single sign-on for IBM Case Manager, you must configure your web application server for SiteMinder.

- Install WebSphere Application Server and enable application level security.
- For WebSphere Application Server Network Deployment systems, install the WebSphere Application Server Network Deployment Manager and configure application level security. Configure your system according to your needs and requirements.
- Install and configure IBM FileNet P8 Content Platform Engine.
- Install and configure IBM Content Navigator with SiteMinder. For more information, refer to the following technote Configuring single sign-on for IBM Content Navigator by using CA eTrust SiteMinder (IBM FileNet P8 on WebSphere Application Server.

Procedure

To configure SSO support for IBM Case Manager by using SiteMinder:

1. You will need to create protected realms and rules for IBM Case Manager on the SiteMinder policy server. Two protected realms are needed for each of the reverse proxy servers and the IBM Case Manager server. For each protected realm, create a rule with the actions that are specified in the following table and set the rule to enabled unless otherwise specified.

Table 16. SiteMinder policy server protected realms

Realm	Agent	Realm Resource Filter	Authentication Scheme	Web Agent Actions	Resource
CaseManager	Server	`/CaseManager`	Basic	Get, Post, Put	/*
CaseManager	Proxy server	`/CaseManager`	Basic	Get, Post, Put	/*
CaseBuilder	Server	`/CaseBuilder`	Reverse proxy form	Get, Post, Put	/*
CaseBuilder	Proxy server	`/CaseBuilder`	Reverse proxy form	Get, Post, Put	/*
ICMClient	Server	`/ICMClient`	Basic	Get, Post	/*
ICMClient	Proxy server	`/ICMClient`	Basic	Get, Post	/*
CaseManagerHelp	Server	`/CaseManagerHelp`	Basic	Get, Post	/*
CaseManagerHelp	Proxy server	`/CaseManagerHelp`	Basic	Get, Post	/*

2. Add the rules that you created for each realm to be part of the appropriate policy. There should be two polices created in the policy server: one for the proxy server and one for the IBM Case Manager server. If a rule is created for the proxy server agent, add the rule to the proxy server policy. If the rule is created against the IBM Case Manager server agent, then add it to the IBM Case Manager server policy.
3. After you have completed the protected realms and rules and added them to the correct policies, restart the SiteMinder policy server, the HTTP reverse proxy server, and the WebSphere Application Server on which IBM Case Manager and IBM Content Navigator are deployed. For highly available clustered systems, restart the IBM Content Navigator cluster, the IBM HTTP Server, and the node agent for each node in the cluster.
4. Install IBM Case Manager, and run all of the configuration and deployment tasks that apply to your system.
5. Restart the application server where IBM Case Manager is deployed.

   Important: Highly available cluster systems: In the WebSphere Application Server Network Deployment console, ensure that you add the IBM HTTP

Server to each of the IBM Case Manager web applications in the **Manage Modules** section. Restart the IBM Case Manager cluster, the IBM HTTP Server, and the node agent for each node in the cluster.

Related tasks:

"Verifying your SSO deployment" on page 113

Related information:

"Troubleshooting CA eTrust SiteMinder single sign-on configuration" on page 197

Configuring IBM Case Manager to support SSO through Kerberos SPNEGO

You can configure IBM Case Manager to support single sign-on (SSO) authentication through Kerberos SPNEGO with an FileNet P8 repository and WebSphere Application Server.

Before you begin

Before you configure single sign-on for IBM Case Manager, you must configure your web application server for SPNEGO.

- Configure your Active Directory domain and configure all of the client workstations as members of the same domain as your Active Directory server. If you have a more complex configuration, you can configure the client workstations as members of a different domain and then cross certify the servers.
- Install WebSphere Application Server and enable application level security.
- For WebSphere Application Server Network Deployment systems, install the WebSphere Application Server Network Deployment Manager and configure application level security. Configure your system according to your needs and requirements.
- Install and configure IBM FileNet P8 Content Platform Engine.
- Install and configure IBM Content Navigator with SPNEGO. For more information, refer to the following technote Configuring single sign-on for IBM Content Navigator by using SPNEGO/Kerberos (IBM FileNet P8) on WebSphere Application Server.
- Install IBM Case Manager.

Procedure

To configure SSO support for IBM Case Manager by using Kerberos SPNEGO:

1. Open the IBM Case Manager `configmr.ini` file in a text editor. The `configmr.ini` file can be found in the *drive*`\Program Files\IBM\CaseManagement\configure` directory or *drive*`\Program Files (x86)\IBM\CaseManagement\configure` directory by default.
2. Add the following parameters to the `configmr.ini` file.

   `Djava.security.auth.login.config`
   The location of the *WAS_PROFILE_HOME*`/properties/wsjaas_client.conf` file.

   `Dicm.spnego.enable`
   Should be set to TRUE.

   `Dicm.spnego.serverSPN`
   The Kerberos Service server principal name (SPN).

   For example:

```
- Djava.security.auth.login.config=
C:/Program Files/IBM/WebSphere/AppServer/profiles/AppSrv01/properties/
wsjaas_client.conf
- Dicm.spnego.enable=true
- Dicm.spnego.serverSPN=HTTP/kerwassrv.kertestdomain.com@KERTESTDOMAIN.COM
```

3. Optional: AES encryption is the default encryption specification used to generate the Kerberos keytab file on Windows 2008 Server and Windows 2008 Server R2 systems. AES encryption is currently not fully supported by the IBM Case Manager configuration tool. In order to use AES encrypted Kerberos keytabs in your IBM Case Manager, Windows 2008 Server and Windows 2008 Server R2 users must patch the supported Java Runtime Environment (JRE) to support unlimited key strength in the Java Cryptography Extension (JCE) package used by the IBM Case Manager configuration tool.
   a. Back up the `US_export_policy.jar` and `local_policy.jar` files that can be found in the *`CaseManagerInstallLocation`*`\java\sdk\jre\lib\security` directory.
   b. Ensure that the IBM Case Manager configuration tool is stopped.
   c. Download the unlimited strength encryption security policy files (for WebSphere Application Server only) to the *`CaseManagerInstallLocation`*`\java\sdk\jre\lib\security` directory.
   d. Disable pre-authentication with Kerberos for the LDAP user that is specified as the IBM Content Navigator administrator in the IBM Case Manager configuration tool. Disable Kerberos pre-authentication for the user account in Microsoft Active Directory that the IBM Case Manager configuration tool is using to connect to IBM Content Navigator.
4. Optional: If you are an AES encryption user, you can generate a new Kerberos keytab file to use DES encryption instead of AES encryption specifically for the IBM Case Manager configuration tool. You will also have to create a new corresponding kerberos configuration file for the new keytab file that you have created. Create the keytab file with DES encryption by entering the following command:

   ```
   ktpass -out keyfile_name
   -princ HTTP/fully_qualified_HTTP_Server_host_name@AD_DOMAIN_NAME
   -pass password -ptype KRB5_NT_PRINCIPAL -crypto DES-CBC-MD5
   ```

   You must specify the path to the new Kerberos configuration file and keytab file using the `java.security.krb5.conf` JVM property in the IBM Case Manager configuration tool `configmgr.ini` file. For example, if your kerberos configuration file (`krb5.ini` file) is located in the `C:\SSO\` directory, then you need to add the following line to the `configmgr.ini` file:

   ```
   -Djava.security.krb5.conf=C:/SSO/krb5.ini
   ```

5. Run the IBM Case Manager configuration tool. Create a new deployment on WebSphere Application Server.
6. Run all of the configuration and deployment tasks that apply to your IBM Case Manager system.
7. Restart the application server where IBM Case Manager is deployed.
8. Optional: Highly available cluster systems: In the WebSphere Application Server Network Deployment console, ensure that you add the IBM HTTP server to each of the IBM Case Manager web applications in the Manage Modules section of the console. Restart the IBM Case Manager cluster, the IBM HTTP Server, and the node agent for each node in the cluster.

Related tasks:

"Verifying your SSO deployment" on page 113

Related information:

"Troubleshooting Kerberos SPNEGO single sign-on configuration" on page 197

Configuring IBM Case Manager to support SSO through IBM Security Access Manager for Web

You can configure IBM Case Manager to support single sign-on (SSO) authentication through IBM Security Access Manager for Web.

Before you begin

Before you configure SSO support, you must complete these tasks:

1. Install, configure, and verify the deployment of your IBM Content Navigator environment with IBM Security Access Manager for Web by completing the predeployment tasks.
2. Install, configure, and verify the deployment of IBM Case Manager.

About this task

The steps described in this topic should be considered as guidance only. The steps might be different in your environment and you might have to modify them depending on your requirements. Consult with your administrator for your environmental requirements and modifications.

Procedure

To configure SSO support for IBM Case Manager by using IBM Security Access Manager for Web:

1. Configure the permissions for IBM Case Manager users.
   a. Log in to the IBM Security Access Manager for e-business web console and navigate to **IBM Security Access Manager** > **Web Portal Manager** > **Groups** > **Create Group**.
   b. Enter a group name for your IBM Case Manager users, for example, `icm-users` and a valid Registry GUID for the group, for example, cn=icm-users,cn=SecurityGroups,secAuthority=ISAMDomain,dc=local.
   c. Add your IBM Case Manager users such as administrator, testid, and any others to the `icm-users` group.
   d. Navigate to **Object Space** > **Browse Object Space**.
   e. Expand the object tree to locate the default access list for Webseal, `default-webseal`.
   f. Under Groups, click **Create Group**, and create a group named `icm-users`.
   g. Add the permissions for the IBM Case Manager users.
   h. Open the `default-webseal` access list and click **Create** to create an ACL entry. Check all required permissions for the entry type group and the `icm-users` group.
2. Create junctions to the IBM Case Manager IBM HTTP Server. Start the **pdadmin** utility and create transparent junctions for all the paths for IBM Case Manager. At a minimum, create junctions for all of the following paths:
   - `CaseForms/`
   - `CaseBuilder/`
   - `CaseManagerHelp/`
   - `CaseManager/`

- `ICMClient/`

For example, the following **pdadmin** command creates the junction to IBM Case Manager:

```
pdadmin server task instance1-webseald-iamdemo.tivoli.com create
  -t tcp -h 9.119.90.107 -p 80 –c iv_creds,iv_user,iv_user_l –b
  supply –x /CaseManager
```

3. Restart the application server where IBM Case Manager is deployed. Restart the WebSEAL server instance.

What to do next

For information about handling the `favicon.ico` file with Mozilla Firefox, see Handling the favicon.ico file with Mozilla Firefox.

Configuring IBM Case Manager to support SSO through SAML

You can configure IBM Case Manager to support single sign-on (SSO) authentication through Security Assertion Markup Language (SAML).

Before you begin

Before you configure single sign-on for IBM Case Manager, you must configure your web application server for SAML.

- Install and configure IBM FileNet P8Content Platform Engine.
- Install and configure IBM Content Navigator with SAML. For more information, see Configuring single sign-on for IBM Content Navigator by using Security Assertion Markup Language (SAML) on WebSphere Application Server.

About this task

In this procedure, IBM Tivoli Federated Identity Manager is used as the identity provider.

Procedure

To configure SSO support for IBM Case Manager by using SAML:

1. In WebSphere Application Server, enable your system to use the SAML web single sign-on (SSO) feature. Enable SAML TAI by using the WebSphere Application Server administrative console.

   The following table lists sample information to specify for the custom properties for IBM Case Manager when you use IBM Tivoli Federated Identity Manager as the identity provider. This sample information assumes that you already configured IBM Content Navigator and Task Manager custom properties, hence the numbering convention.

Name	Value
sso_3.sp.acsUrl	https://myproxyserver.mydomain.com/samlsps/acs
sso_3.sp.idMap	localRealm

Name	Value
sso_3.sp.login.error.page	https://myproxyserver.mydomain.com/sps/SAMLforP8/saml20/logininitial?NameIdFormat=Email&PartnerID=https://myproxyserver.mydomain.com/samlsps/acs&Target=https://myproxyserver.mydomain.com/CaseBuilder

2. Create a partner service on your Identity Provider (IdP) for your Service Provider (SP) and import the partner service metadata. For instructions, see Configuring single sign-on (SSO) partners. After you add the identity provider as a partner, the SAML configuration looks like the following example:

Name	Value
sso_3.sp.acsUrl	https://myproxyserver.mydomain.com/samlsps/acs
sso_3.idp_1.certAlias	TFIM
sso_3.idp_1.entityID	https://myproxyserver.mydomain.com/sps/SAMLforP8/saml20
sso_3.idp_1.singleSignOnUrl	https://myproxyserver.mydomain.com/sps/SAMLforP8/saml20/login
sso_3.sp.idMap	localRealm
sso_3.sp.login.error.page	https://myproxyserver.mydomain.com/sps/SAMLforP8/saml20/logininitial?NameIdFormat=Email&PartnerID=https://myproxyserver.mydomain.com/samlsps/acs&Target=https://myproxyserver.mydomain.com/CaseBuilder
sso_3.sp.filter	request-URL%=CaseBuilder

   Configure the WebSphere Application Server security context if required.

   After you complete the configuration, restart the IdP application server and the SP application server on which IBM Case Manager is to be deployed. For highly available cluster systems, restart the IBM Case Manager cluster, the web server, and the node agent for each node in the cluster.

3. Install IBM Case Manager and run all the configuration and deployment tasks that apply to your system.

   Important: When you run the IBM Case Manager configuration tool tasks, enter the HTTPS proxy protocol rather than the HTTP proxy protocol.

4. Restart the application server on which IBM Case Manager is deployed.
5. Optional: Highly available cluster systems: In the WebSphere Application Server Network Deployment console, ensure that you add the IBM HTTPS server to each of the IBM Case Manager web applications in the Manage Modules section of the console. Restart the IBM Case Manager cluster, the IBM HTTPS Server, and the node agent for each node in the cluster.
6. Verify your deployment of IBM Case Manager with SAML SSO. Open a browser window and enter any of the following URLs:

Application	URL
Case Manager Client	https:// *myproxyserver.mydomain.com*/ navigator/?desktop=icm
IBM Case Manager administration client	https:// *myproxyservermydomain.com*/ navigator/?desktop=icmadmin
Case Manager Builder	https:// *myproxyservermydomain.com*/ CaseBuilder

Ensure that you are redirected to the SAML login form and that you can log in to the application.

Verifying your SSO deployment

After you have configured single sign-on, you should verify that it has been set up correctly by connecting to systems and ensuring that no additional login credentials are requested.

Procedure

To verify that IBM Case Manager was successfully deployed in your SSO environment, enter the following URLs in your web browser:

- For an IBM Case Manager Development profile single server system, enter the following URLs:
  - `http://fully_qualified_IBM_Case_Manager_server_name:port/CaseBuilder`
  - `http://fully_qualified_IBM_Case_Manager_server_name:port/?desktop=icm`
  - `http://fully_qualified_IBM_Case_Manager_server_name:port/?desktop=icmadmin`
- For an IBM Case Manager Development profile single server system in an IBM Security Access Manager SSO environment, enter the following URLs:
  - `http://fully_qualified_ISAM_server_name/CaseBuilder`
  - `http://fully_qualified_ISAM_server_name/navigator/?desktop=icm`
  - `http://fully_qualified_ISAM_server_name/navigator/?desktop=icmadmin`
- For an IBM Case Manager Development profile highly available system, enter the following URLs:
  - `http://fully_qualified_HTTP_Server_name/CaseBuilder`
  - `http://fully_qualified_HTTP_Server_name/navigator/?desktop=icm`
  - `http://fully_qualified_HTTP_Server_name/navigator/?desktop=icmadmin`

  If you are verifying Tivoli Access Manager for e-business or IBM Security Access Manager single sign-on configurations, use those fully qualified server names instead of *fully_qualified_HTTP_Server_name*.
- For an IBM Case Manager Production profile single server system, enter the following URLs:
  - `http://fully_qualified_IBM_Case_Manager_server_name:port/?desktop=icm`
  - `http://fully_qualified_IBM_Case_Manager_server_name:port/?desktop=icmadmin`
- For an IBM Case Manager Production profile single server system in an IBM Security Access Manager SSO environment, enter the following URLs:
  - `http://fully_qualified_IBM_Case_Manager_server_name/navigator/?desktop=icm`
  - `http://fully_qualified_IBM_Case_Manager_server_name/navigator/?desktop=icmadmin`

- For an IBM Case Manager Production profile highly available system, enter the following URLs:
  - `http://fully_qualified_HTTP_Server_name/navigator/?desktop=icm`
  - `http://fully_qualified_HTTP_Server_name/navigator/?desktop=icmadmin`

  If you are verifying IBM Security Access Manager single sign-on configurations, use that fully qualified server name instead of *fully_qualified_HTTP_Server_name*.

Related tasks:

"Configuring IBM Case Manager to support SSO through Kerberos SPNEGO" on page 108

"Configuring IBM Case Manager to support SSO through CA eTrust SiteMinder" on page 106

"Configuring IBM Case Manager to support SSO through IBM Tivoli Access Manager for e-business" on page 104

Migrating and deploying case management solutions

After you develop and test a case management solution, you can migrate the solution to another environment. After you migrate a solution to a development environment, you can edit, deploy, and test the solution. After you migrate a solution to the production environment, you can deploy the solution to make it available to your case workers.

Solution migration and deployment

You can migrate a solution from one development environment to another development environment, a test environment, or a production environment. After you develop and test a case management solution, you must deploy the solution in the production environment to make the solution available for your case workers.

When you *migrate* a solution, you move the solution definition data and its related assets to a different environment. When you *deploy* a solution, you make the solution operational in the target environment.

Several types of assets must be exported from the development environment and imported into the target environment. Some assets, such as class definitions and property templates, are usable immediately after migration. Other assets, like workflow definitions, must be deployed to become usable. After migration, the various assets are combined to re-create the solution in the target environment.

Different tools are required to migrate and deploy different assets:

IBM Case Manager assets
Use the IBM Case Manager administration client to migrate the solution and IBM Case Manager assets from one environment to another. These assets include assets that were created in Case Manager Builder when the solution was designed, such as the solution definition, Process Engine configuration, and solution pages.

Other IBM FileNet P8 assets
If your solution package contains assets that were created with other FileNet P8 tools, use FileNet Deployment Manager and Process Configuration Console to migrate the assets from one environment to another. These assets include classes, properties, workflow definitions, workflow system component queues, and content-based objects like forms, search templates, and form templates.

Other IBM and external assets
If your solution package includes assets that were developed outside of IBM Case Manager and FileNet P8 tools, consult with your solution developer for migration assistance. These assets might include assets that are managed by other IBM products and tools or assets that are managed by external products and tools. Examples include analytics, rules, data services, custom widgets, and custom deployable code.

Migration and deployment task flow

The following steps and diagram depict the general task flow for migrating and deploying a solution:

1. Before you migrate a solution, you must test the solution and ensure that the solution works correctly in the development environment.
2. A solution package consists of assets that are stored in the solution folder in a case management design object store. You use the IBM Case Manager administration client to export the solution package from the development environment.
3. If the solution includes solution application assets that were created with other FileNet P8 tools, use FileNet Deployment Manager and Process Configuration Console to export the assets from the development environment.
4. If the solution includes assets that are managed by other IBM products or tools or external products or tools, use tools and processes that are native to those products and tools to migrate the assets from the development environment.
5. Use the IBM Case Manager administration client to import the previously exported solution package to the staging object store of the test or production environment. (If you migrate a solution from one development environment to another, import the solution package to the design object store of the target development environment.)
6. If you exported solution application assets that are managed by other FileNet P8 tools, use FileNet Deployment Manager and Process Configuration Console to import the assets to the test or production environment. Importing these assets also deploys the assets in the target environment.
7. Use the IBM Case Manager administration client to deploy the migrated solution in the test or production environment.
8. If you exported assets that are managed by other IBM products or tools or external products or tools, use tools and processes that are native to those products and tools to make the assets operational in the test or production environment.
9. Depending on the solution application, you might need to configure the environment after you deploy the solution. For example, you might need to import security settings and audit settings. If the solution is translated, you must migrate the translated user interface elements.
10. Test the solution to ensure that it works correctly before you release the solution to your case workers.

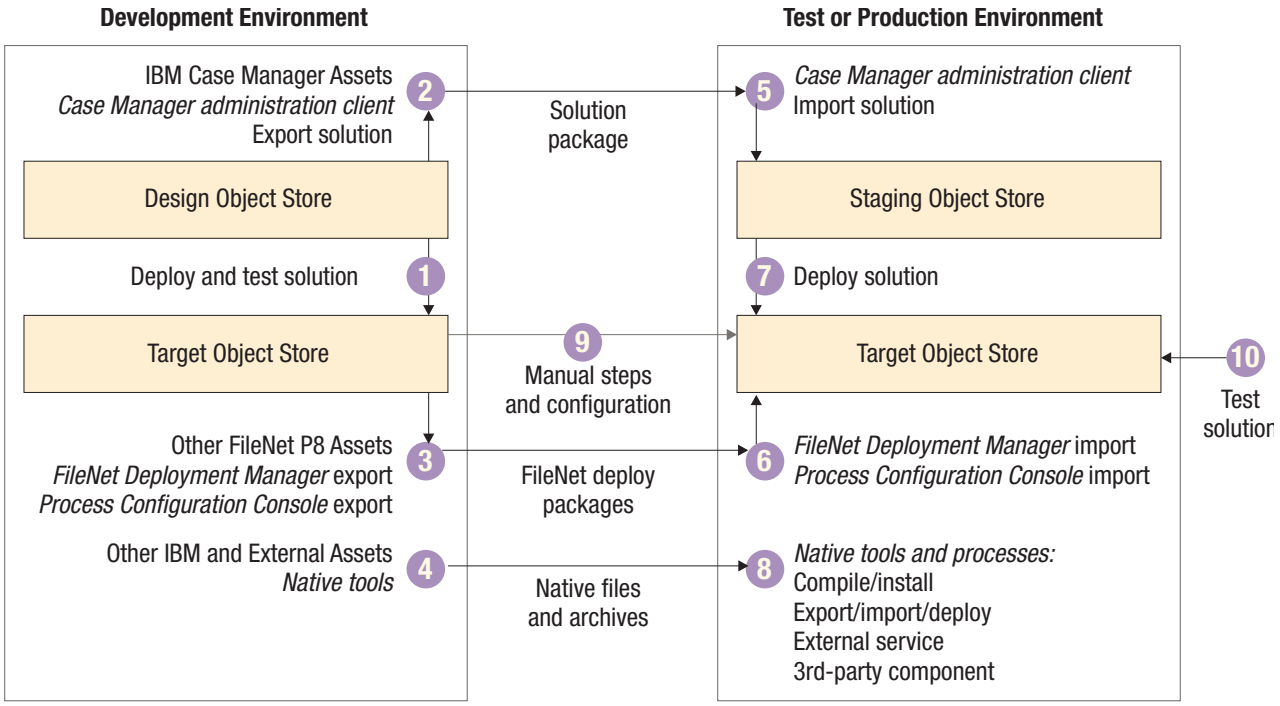


Figure 4. Migrating solution assets from one environment to another

Preparing for solution migration

To help you prepare for migration, identify and collect information about the solution assets that you want to migrate. In addition, prepare a comprehensive set of migration and deployment instructions that are tailored for your environment and solution applications. If your solution package includes assets that are managed by FileNet P8, you must create the FileNet Deployment Manager deployment tree and environment definition.

"Identifying solution assets for migration"

"Preparing customized migration and deployment instructions" on page 127

"Preparing the system configuration for migration" on page 129

Related tasks:

"Preparing the design environment" on page 7

Identifying solution assets for migration

Solution assets are components that comprise a solution, such as definition files, workflow collections, and pages. When you migrate your solution from one environment to another, you must ensure that you migrate all of the assets that are associated with your solution.

About this task

The first step when you prepare to migrate a solution is to identify and document all of the assets that are to be migrated. This assessment includes the following types of assets:

Solution assets
IBM Case Manager assets. These assets are created when the solution is

designed in Case Manager Builder, and they are bundled together when a solution package is created in the IBM Case Manager administration client.

Solution application assets
Extra assets that are packaged by using tools that are local to the product component that is used to create them:

- Other FileNet P8 assets. These assets are associated with the solution but managed by other FileNet P8 tools. These assets must be migrated and deployed through FileNet Deployment Manager and Process Configuration Console.
- Other IBM and external assets. These assets are developed outside of IBM Case Manager and FileNet P8 tools. Manual changes are required to migrate and deploy these types of assets.

"Solution assets"

"Solution application assets" on page 120

"Obtaining a solution description document" on page 123

"Obtaining a list of object store properties and document types" on page 124

"Solution List page" on page 126

Solution assets

Solution assets are created in the IBM Case Manager development environment when you design the solution. When you export a solution package in the administration client, these assets are included in the package.

A *solution definition* refers to the solution assets as defined in the design object store. A *solution package*, which is created when you export the solution, refers to the archive file of the solution.

Solution Document Generator tool

When you migrate your solutions from one environment to another, ensure that you migrate all of the assets that are associated with your solution. You can generate documentation about the IBM Case Manager solution assets by running a command-line tool, the Solution Document Generator.

In Case Manager Builder, the solution designer can capture requirements directly into this tool. You can then generate a document that presents the organization of the solution and its contents in an easy-to-read format. This solution description document provides a way to communicate and share the configuration details of the solution for review, discussion, and analysis.

IBM Case Manager assets

The development environment is typically in a dedicated IBM FileNet P8 domain and includes a design object store in which solutions are stored. Each time that you edit and save the solution in Case Manager Builder, a new version of the assets is created. All of the versions of the assets are saved in the design object store, and each version of the assets has a unique ID. When you deploy a solution, the latest version of the solution assets is deployed with the solution.

When you export a solution by using the IBM Case Manager administration client, the following solution assets are included in the solution package.

Solution asset	Defined by using	Resides in	Migration tool	Deployment tool
Solution definition file	Case Manager Builder	Design object store	IBM Case Manager administration client, IBM Case Manager configuration tool	IBM Case Manager administration client, IBM Case Manager configuration tool, Case Manager Builder
Process Engine configuration file	Case Manager Builder, Process Designer	Design object store	IBM Case Manager administration client, IBM Case Manager configuration tool	IBM Case Manager administration client, IBM Case Manager configuration tool, Case Manager Builder
Solution workflow collection	Case Manager Builder, Process Designer	Design object store	IBM Case Manager administration client, IBM Case Manager configuration tool	IBM Case Manager administration client, IBM Case Manager configuration tool, Case Manager Builder
Task workflows	Case Manager Builder, Process Designer	Design object store	IBM Case Manager administration client, IBM Case Manager configuration tool	IBM Case Manager administration client, IBM Case Manager configuration tool, Case Manager Builder
Pages	Case Manager Builder	Design object store	IBM Case Manager administration client, IBM Case Manager configuration tool	IBM Case Manager administration client, IBM Case Manager configuration tool, Case Manager Builder
Business rules	Case Manager Builder	Design object store	IBM Case Manager administration client, IBM Case Manager configuration tool	IBM Case Manager administration client, IBM Case Manager configuration tool, Case Manager Builder
Case instance security	IBM Case Manager administration client	Design object store	IBM Case Manager administration client	IBM Case Manager administration client

Solution asset	Defined by using	Resides in	Migration tool	Deployment tool
Case history audit configuration	IBM Case Manager administration client	Design object store	IBM Case Manager administration client	IBM Case Manager administration client

If you want to migrate business rules to IBM Operational Decision Manager, use the IBM Case Manager administration client to export the rules. For more information, see Exporting business rules to IBM Operational Decision Manager.

Solution application assets

Solutions can include assets that are not included in the solution package that is created in the IBM Case Manager administration client. These extra assets, called *solution application assets*, are created and managed by non-IBM Case Manager tools.

Examples of solution application assets include forms, image objects, custom rules, custom servlets, widgets, and reporting templates. When you migrate your solutions from one environment to another, ensure that you migrate all of the solution application assets that are associated with your solution.

If your solution is translated, you must migrate the translated user interface in your case management application by exporting the translated assets from the source domain and deploying them in the target domain. For more information, see "Migrating the translated user interface elements of your case management application" on page 156.

Other FileNet P8 assets

The following assets are stored in Content Platform Engine or other components that are managed by FileNet P8 tools.

Solution asset	Defined by using	Resides in	Migration tool	Deployment tool
Reused Content Engine classes and properties	Administration Console for Content Platform Engine	Target object store	FileNet Deployment Manager	FileNet Deployment Manager
Reused queues and component queues	Process Configuration Console	Target object store	Process Configuration Console and FileNet Deployment Manager	Process Configuration Console
Content Engine marking sets	Administration Console for Content Platform Engine	FileNet P8 domain	FileNet Deployment Manager	FileNet Deployment Manager
Content Engine event subscription	Administration Console for Content Platform Engine	Target object store	FileNet Deployment Manager	FileNet Deployment Manager

Solution asset	Defined by using	Resides in	Migration tool	Deployment tool
Content Engine event code module	Administration Console for Content Platform Engine	Target object store	FileNet Deployment Manager	FileNet Deployment Manager
Content Engine event workflow	Process Designer	Target object store	FileNet Deployment Manager	FileNet Deployment Manager
IBM FileNet eForms for P8 form template	IBM FileNet eForms for P8 designer	Target object store	FileNet Deployment Manager	FileNet Deployment Manager
IBM Forms form template	IBM Forms designer	Target object store	FileNet Deployment Manager	FileNet Deployment Manager
IBM Content Navigator search that is stored in the FileNet P8 repository	IBM Content Navigator	Target object store	FileNet Deployment Manager	FileNet Deployment Manager

Other IBM and external assets

The items in this table represent assets that are managed other IBM products and tools, and external assets, such as custom widgets and services, that are managed by external products and tools.

Solution asset	Defined by using	Resides in	Migration tool	Deployment tool
IBM Content Manager item types	IBM Content Manager system administration client	IBM Content Manager library server	IBM Content Manager system administration client	IBM Content Manager system administration client
IBM Content Navigator desktop	IBM Content Navigator	IBM Content Navigator configuration database	IBM Content Navigator administration tool	IBM Content Navigator administration tool
IBM Operational Decision Manager rules project (formerly known as WebSphere ILOG® JRules BRMS)	IBM Operational Decision Manager Rule Designer	IBM Operational Decision Manager Decision Center		
IBM Operational Decision Manager rules application	IBM Operational Decision Manager Rule Designer	Application server		IBM Operational Decision Manager, IBM Case Manager administration client, FileNet Deployment Manager

Solution asset	Defined by using	Resides in	Migration tool	Deployment tool
Reused IBM Business Process Manager processes	IBM Business Process Manager Process Designer	Process center, Process server	Process center administration tool	Process center administration tool
IBM Watson Content Analytics	IBM Watson Content Analytics administration console	File	IBM Watson Content Analytics administration console	IBM Watson Content Analytics administration console
Case Analyzer	Process Task Manager	OLAP database	Process Task Manager	Microsoft SQL Server OLAP Services
Cognos® Real-time Monitoring	Cognos Real-time Monitoring Workbench	Database for Cognos Real-time Monitoring	Cognos Real-time Monitoring Workbench	
External Data Service	External tool	External tool	External tool	External tool
Email templates that are checked in as documents		Target object store		FileNet Deployment Manager
Widget: page	External tool such as a JavaScript editor, a Java editor, or a compression utility	Custom widgets package	Not applicable. Instead of migrating, you build the custom widgets package.	IBM Case Manager configuration tool For a custom widgets package, you can also use the IBM Case Manager administration tool.
Widget: property editor	External tool such as a JavaScript editor, a Java editor, or a compression utility	Extensions package	Not applicable. Instead of migrating, you build the extensions package.	IBM Case Manager configuration tool
Widget: other	External tool such as a JavaScript editor, a Java editor, or a compression utility	External tool	External tool	External tool

Related concepts:

FileNet P8 assets

Obtaining a solution description document

You, or your business analyst, can generate a solution description document by running the Solution Document Generator from a command line. The solution description document includes a list of all the cases and their assets for a specific solution.

About this task

A solution consists of a set of cases and supporting information, including a definition file that describes the overall structure and contents of the solution, a set of XPDL files describing workflows that are associated with the cases in the solution, and a Process Engine configuration file that contains the Process Engine configuration details, such as queue, role, in-basket, roster, event log, application space, and step processor definitions for the solution.

The Solution Documentation Generator creates a solution description document that provides a summary of the contents of the solution definition file (SDF), XPDL files, and the Process Engine configuration file. The solution description document does not list rules, views, and pages.

When you design solutions, you can use the solution description document to view the organization of the solution and its contents in an easy-to-read format that can be shared with case workers and customers.

You can create a solution description document for only one solution at a time. You can choose from one of the following types of output: PDF, Microsoft Word, or XHTML.

Procedure

To generate a solution description document:

1. Navigate to the Solution Documentation Generator location:

Operating system	Location
AIX	`/opt/IBM/CaseManagement/docGenerator`
Linux	`/opt/IBM/CaseManagement/docGenerator`
Linux for System z	`/opt/IBM/CaseManagement/docGenerator`
Windows	`C:/Program Files/IBM/CaseManagement/docGenerator/`

   Restriction: For the Solution Documentation Generator to successfully create solution description documents, the IBM Case Manager installation path cannot contain special non-English characters or symbols.

2. Open the `docGenerator.properties` file in a text editor and define your IBM Case Manager environment.
   a. For the `ceURI` property, enter the full URI of the Content Engine server. For example, http://*localhost*:9080/wsi/FNCEWS40TOM.
   b. For the `objectStoreName` property, enter the name of the design object store that contains the solution that you want to generate a solution description document for.
   c. For the `solutionName` property, enter the name of the solution that you want to generate a description document for.

d. For the `outputFormat` property, enter the output format for the solution description document.

   PDF To get an Adobe Acrobat PDF file.

   Word To get a Microsoft Word Rich Text Format (RTF) document.

   HTML
   To get an XHTML file.

e. For the `outputLocation` property, enter the directory location where you want the solution description document to be created.

f. Optional: For the `antOpts` property, enter the maximum memory to be allocated to the JVM for a large solution.

The following example shows an example of a `docGenerator.properties` file:

```
ceURI = http://myServer:9080/wsi/FNCEWS40MTOM
objectStoreName = CMDOS
solutionName = MySolution
outputFormat = PDF
outputLocation = C:/IBM/CaseManagement/docGenerator/output
antOpts = -Xmx2000m -Dmax JavaMemory=2000m
```

Tip: For the **`outputLocation`**, you must use a forward slash (/) to separate folder names in the properties file regardless of your operating system type.

3. Open a command prompt and run the Solution Document Generator. You can append a parameter to the command to check in the generated document into the FileNet repository: **`checkin`**.

   The **`checkin`** parameter checks in the solution description document into the same object store in the solution folder. By checking in the solution description document into the same folder as the solution, you can iteratively monitor how the solution design changes.

Operating system	Command
AIX	`docgen.sh`
Linux	`docgen.sh`
Linux for System z	`docgen.sh`
Windows	`docgen.bat`

   For example, enter `docgen.bat -checkin`

4. At the prompt, enter a user name and password that can retrieve and add content to Content Platform Engine.

Results

The Solution Document Generator produces a document with the name of the solution and an extension that is appropriate for the output format. The document is added to the location that is specified in the properties file, for example: `C:/IBM/CaseManagement/docGenerator/Output/MySolution.pdf`. The document is also checked into the design object store in the solution folder if you provide a **`checkin`** parameter.

Obtaining a list of object store properties and document types

To help you prepare for solution migration, you or your business analyst can generate text files that provide information about all object store properties and document types in a development environment target object store.

About this task

You can use the IBM Case Manager configuration tool to create two comma-separated value text files, `PropertyTemplates.csv` and `DocumentTypes.csv`.

The `PropertyTemplates.csv` file contains the following values for the properties in the object store:

- Property Template Display Name
- Symbolic Name
- Data Type
- Description
- Cardinality (single value or multi-value choice list)
- Default Value
- Min Value
- Max Value
- Max Length
- Choice List
- Required
- Hidden

The `DocumentTypes.csv` file contains the following values for the document types in the object store:

- Display Name
- Symbolic Name
- Descriptive Text
- Is Hidden
- Is Persistent
- Properties (symbolic names of properties associated with this document type)

Creating a list of object store properties and document types applies only in the development environment.

Procedure

To create a list of the object store properties and document types in an object store:

1. Start the configuration tool by running one of the following commands:

Operating system	Command
AIX	1. Change to the *_install_path*`/configure` directory. *_install_path* is the location where IBM Case Manager is installed, for example, `/opt/IBM/CaseManagement`. 2. Run the following command: `./configmgr`

Operating system	Command
Linux	1. Change to the *_install_path*/configure directory. *_install_path* is the location where IBM Case Manager is installed, for example, /opt/IBM/CaseManagement. 2. Run the following command: ./configmgr
Linux for System z	1. Change to the *_install_path*/configure directory. *_install_path* is the location where IBM Case Manager is installed, for example, /opt/IBM/CaseManagement. 2. Run the following command: ./configmgr
Windows	Perform one of the following actions: • Click **Start** > **All Programs** > **IBM Case Manager** > **Case Manager Configuration Tool**. • Run the following command: *_install_path*\configure\configmgr.exe *_install_path* is the location where IBM Case Manager is installed, for example, one of the following directories: – C:\Program Files\IBM\CaseManagement – C:\Program Files (x86)\IBM\CaseManagement

2. Click **Tools** > **List Property Templates and Document Types** to create the list of properties by using the wizard.
3. Provide copies of the CSV files to your business analysts who design solutions in Case Manager Builder. You can open the CSV files in a text editor, a spreadsheet, or other program to review the list of available document types or property templates and their settings.

Solution List page

The IBM Case Manager Solution List page displays the solutions that are deployed to all object stores. You can see each solution's status, description, FileNet P8 target environment, and Case Manager Client URL.

To open the Solution Deployment Status page in a web browser, go to http://*server name*:*port number*/*Web App Root Path*/CASEREST/v1/solutions, where the *server name* is the system where IBM Case Manager was installed.

For each deployed solution, the following details are displayed:

Object store
The object store where the solution is deployed. This can be a production environment or a development environment where the solution is being designed.

Solution name
The name of the solution that was defined by the business analyst in the Case Manager Builder.

Status The solution status can be initiated, completed, or failed.

Description
The description of the solution that was defined by the business analyst in the Case Manager Builder.

FileNet P8 target environment
The target environment is set in the Define a Target Environment window in the IBM Case Manager administration client for each target environment.

A target environment is associated with a specific isolated region in the workflow database. The isolated region is defined by an administrator by using Administration Console for Content Platform Engine.

Case Manager Client URL
The web address at which business analysts or end users can access Case Manager Client.

Preparing customized migration and deployment instructions

To prepare for migration, create a comprehensive set of instructions that are tailored for your environment and solution applications. The instructions serve as a roadmap for the process to follow when you migrate a solution application from the development environment to a test or production environment.

About this task

Ensure that the instructions include the required tasks, their order of execution, configuration details and options, and the roles that are involved in the processes, including information about required system privileges. The following types of information are examples of solution migration and deployment process information to include.

Tips:

- To ensure that assets are imported in the correct order during deployment, you must understand the dependencies between assets. Consult with your development team and system administrators to develop a detailed plan for all types of assets that must be exported and imported.
- Although this documentation can be created when the deployment process begins, it is more efficient and produces a more complete description if the developers and designers complete the documentation as part of the development process.

Solution packages
Name and location of the solution package that was created when the solution was exported by using the IBM Case Manager administration client. If a solution package was not yet created, include the solution information to must be specified when the solution is exported. Also include the name and location of any other solution packages that must be deployed before this solution is deployed.

FileNet Deployment Manager information
Instructions for running FileNet Deployment Manager to create the deploy packages of the assets that are managed by FileNet P8 tools. If a deploy package was provided as an input to the migration process, this information is not required.

- Name and location of any existing deployment trees and FileNet Deployment Manager environments with required export manifests. If deployment trees were not already created, information about the

environment and the FileNet P8 assets to export is needed to facilitate creation of the FileNet Deployment Manager environments and export manifests.

- Name of the project area from which to export the assets that are managed by FileNet P8.
- If the **Include all document versions** include option will not be used, note which assets must be deleted or added to the manifest each time to ensure that the correct version of the asset is included in the export. For a description of the export include options that are typically used for IBM Case Manager solution application export, see FileNet Deployment Manager include options for assets
- Which assets must be deployed before or after the solution is deployed, and which assets must be deployed before or after other assets.

Data mapping information

Data maps are used by the IBM Case Manager administration tool and FileNet Deployment Manager to convert the metadata and content of assets that are exported from the source environment to reflect the information that is specific to the target environment. Information is typically needed about the following sets of data maps:

Object stores

The target object store in the project area that the solution is exported from is mapped to the corresponding object store in the target environment to which the solution is to be deployed. If some assets are located in other object stores, note the names of these object stores and the assets that are in each object store.

Security principals

The user or group in the destination environment that is to be assigned the access privileges of a specific principal from the source environment.

Service data

Service data can represent any number of types of configuration data or services. Information about the configuration or services in the source environment is matched to an entry for the destination environment according to the following information:

- By its type as extracted from the metadata and content in the deploy dataset. For example, all services of type PESystemAdministration_F_WebServer in the source map are mapped to services of type PESystemAdministration_F_WebServer in the destination map.
- Labeled source services are matched with destination services that have the same labels and are of the same type. If no destination services have matching labels, the mapping is done by name.
- Any source services that cannot be mapped to a destination service are added to the data map as unmapped services.

System configuration steps

Configuration steps that are required to complete the deployment of the solution or other assets. All configuration information should be included in the solution documentation. For example, include the following information:

- System configuration steps to complete before the solution is deployed, such as establishing a web service.

- Postrequisite steps to complete after the solution is deployed, such as setting up the printers that are expected to be available as a part of the operating environment of the case worker.
- Security configuration details
- Audit definition configuration details

Destination environment
Information about the destination environment, such as the following information:

- Assets that are not directly managed by IBM Case Manager or FileNet P8 tools, such as rules or custom services.
- Special backup considerations, such as for assets that are managed in an organization-wide technology such as IBM Operational Decision Manager.

Post-migration steps
Information about one-time tasks or special tools that are needed to alter existing case instances to reflect the redeployed solution. Also, include a verification plan for testing the various methods and roles that create and modify cases. It is especially important to test integrations with external components that might not have been available in the development or test environments.

Preparing the system configuration for migration

When a solution application is migrated to and deployed into a system for the first time, additional steps might be required to configure the new target environment.

About this task

During redeployment of a solution, some system configuration information might be overwritten and might need to be specified again. However, most configuration steps do not need to be repeated.

"Creating the FileNet Deployment Manager deployment tree"

"Creating the FileNet Deployment Manager environment" on page 130

Creating the FileNet Deployment Manager deployment tree

If your solution package includes assets that are managed by FileNet P8, create a deployment tree for the files to be migrated with FileNet Deployment Manager.

About this task

A deployment tree contains the files that FileNet Deployment Manager creates. A deployment can be between connected or disconnected environments.

Connected environments
One FileNet Deployment Manager instance can access the source and destination environments and is used for the export and import tasks.

Disconnected environments
Different FileNet Deployment Manager instances are used for the export and import tasks. For example, you might have disconnected environments because the source and destination environments are separated by a firewall or the solution application was developed externally.

After you export the solution assets from the source environment by using FileNet Deployment Manager, you must move the deploy package to the destination environment. The package contains the information about the

source environment that is needed to import the package into the destination environment. If the systems are disconnected, the source environment is typically extracted from the deploy package into the deployment tree for the FileNet Deployment Manager instance that is used to import the solution into the destination environment.

If the deployment is connected, only one deployment tree is needed. However, if a deployment is disconnected or different computers are used to import and deploy the solution assets, a deployment tree must be created on each computer.

Procedure

To create a FileNet Deployment Manager deployment tree:

1. Start FileNet Deployment Manager.
2. In the Select Deployment Tree Location window, browse to the folder in which to create the deployment tree.
3. Click **Window** > **PreferencesGeneral options** and set the following options.
   - Clear the **Enable FIPS 140-ready mode** option to allow FileNet Deployment Manager to store passwords as encrypted data. Otherwise, you must enter a password each time you runFileNet Deployment Manager. In addition, clearing this option allows FileNet Deployment Manager to convert embedded passwords for certain service data in a deploy dataset if you enter new passwords for the target service data as a part of the data mapping task. For more information, see About passwords.
   - Verify that the **Export metadata assets created by an AddOn** option is set to **Never**.

Related concepts:

Concepts: About FileNet Deployment Manager

Creating the FileNet Deployment Manager environment

You must create a FileNet Deployment Manager environment definition for each of the development, test, and production environments that are involved in the solution application migration. Environment definitions enable FileNet Deployment Manager to connect to Content Platform Engine.

About this task

Each FileNet Deployment Manager environment can serve as the source environment in one operation and the destination environment in another operation. The inclusion of an environment in a source-destination pair determines whether the environment is being used as a source environment or a destination environment.

Procedure

To create a FileNet Deployment Manager environment

1. Start the FileNet Deployment Manager and ensure that the correct deployment tree is selected.
2. Create the environment definition by clicking **File** > **New Environment**.
3. Define the connection parameters for the environment.
   a. In the deployment tree, double-click the node for the new environment.
   b. On the **Content Platform Engine Connection** tab at the bottom of the window, enter the connection information for Content Platform Engine.

Tip: Select the **Save the password** check box to store the encrypted password.

c. Click **Test Connection**. If FileNet Deployment Manager cannot connect to Content Platform Engine, verify that the specified connection information is correct.

d. In the **PE Connection Point** list, select the connection point that corresponds to the project area or target environment with which this environment is to be used.

e. Click **File** > **Save** to save the connection settings.

Related concepts:

Checklist: Environment definitions

Migrating solutions

To migrate a solution, you export the solution assets that were defined in Case Manager Builder and optionally other solution application artifacts from the development environment. You then import the assets to the new environment.

1. "Exporting IBM Case Manager assets"
2. "Exporting other FileNet P8 assets" on page 135
3. "Exporting other IBM and external assets" on page 140
4. "Importing IBM Case Manager assets" on page 140

Related tasks:

"Exporting a solution package by using the command line" on page 296

"Migrating the translated user interface elements of your case management application" on page 156

Copying IBM Case Manager solutions that are associated with IBM Business Process Manager process applications

Exporting IBM Case Manager assets

To migrate a solution to another environment, you must first export the assets for that solution so that they can be copied to the new environment.

About this task

Solution assets include those assets that were defined for the solution in Case Manager Builder. In addition, your solution might include assets that were created with other IBM FileNet P8 tools, other IBM products or tools, or with non-IBM products or tools.

Typically, you export solution assets that were defined in Case Manager Builder by using the IBM Case Manager administration client.

If IBM Case Manager is integrated with a version control system (VCS), you can extract these assets from the VCS.

"Exporting IBM Case Manager assets from a design object store" on page 132

"Exporting IBM Case Manager assets from a VCS" on page 133

"Exporting the security configuration" on page 134

"Exporting the audit configuration" on page 134

Exporting IBM Case Manager assets from a design object store

You can use the IBM Case Manager administration client to export solution assets from the design object store. This export process creates a solution package that contains all assets that were created for the solution in Case Manager Builder.

Before you begin

The IBM Case Manager administration client can only export a solution package if the solution was committed from Case Manager Builder.

If the solution includes assets or components that are not managed by IBM Case Manager or by FileNet P8 tools, migrate these external assets to the target environment by using native tools and processes as required by the particular solution application asset.

Procedure

To export a solution package:

1. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   `http://`*`server`*`:`*`port`*`/navigator/?desktop=icmadmin`
   `server` is the IBM Content Navigator IP address or fully qualified server name.
   `port` is the IBM Content Navigator port number.
2. In the navigation tree in the left pane, select a design object store and click **Solutions**.
3. On the Solutions page in the right pane, select the solution that you want to export.
4. Click **Actions** > **Export** > **Solution** and complete the wizard steps. After you complete the wizard steps, the solution package ZIP file is created in the folder that you specified.

What to do next

If your solution contains assets that were created in tools other than IBM Case Manager, you must migrate and deploy these other assets with your solution application. For example:

- If your solution contains assets that were created in FileNet P8, use FileNet Deployment Manager to create a deploy package that contains the assets.
- If your solution is associated with an IBM Business Process Manager process application, you must export a snapshot of the process application. Before you import the solution package to the target environment, you must import the process application.
- If your solution includes pages that contain custom widgets, which might not exist in the target environment, you must migrate the widgets before you import the solution package. The pages are included in the `Pages` folder of the exported solution.
- If your solution uses properties that are associated with marking sets and you move the solution to a different environment, you must re-create the marking sets and any property templates that use the marking sets in the target environment. To re-create the marking sets, use the appropriate FileNet P8 tools. When you re-create the properties, you must use the same symbolic name that is used in the source environment.

To migrate the marking sets, use FileNet Deployment Manager to export and import the marking sets but not any property templates, which are created when the solution is deployed by IBM Case Manager.

Related tasks:

"Exporting a solution package by using the command line" on page 296

Exporting IBM Case Manager assets from a VCS

If you delivered solution assets to a version control system (VCS), you can use the delivery label to export the solution assets and solution manifest from the VCS. You then can migrate and deploy the solution assets to a new environment.

About this task

Export only those solution assets and solution manifest that were created for the solution in Case Manager Builder.

Important: Export the solution assets and solution manifest to a directory that is accessible to IBM Content Navigator. When you import the solution, you must specify a directory location that is relative to the IBM Content Navigator application rather than to the system where IBM Case Manager administration client is running.

Procedure

To export IBM Case Manager assets from a VCS:

- Use the graphical user interface of your VCS, if one is provided, to export all the solution assets and the solution manifest that are associated with a specific delivery label.
- Create a script that uses the delivery label to export all the solution assets and the solution manifest from the VCS.

What to do next

Important: Do not edit the solution manifest or the solution files after you export them from the VCS.

If your solution contains assets that were created in tools other than IBM Case Manager, you must migrate and deploy these other assets with your solution application. For example:

- If your solution contains assets that were created in FileNet P8, use FileNet Deployment Manager to create a deploy package that contains the assets.
- If your solution is associated with an IBM Business Process Manager process application, you must export a snapshot of the process application. Before you import the solution package to the target environment, you must import the process application.
- If your solution includes pages that contain custom widgets, which might not exist in the target environment, you must migrate the widgets before you import the solution package. The pages are included in the `Pages` folder of the exported solution.
- If your solution uses properties that are associated with marking sets and you move the solution to a different environment, you must re-create the marking sets and any property templates that use the marking sets in the target

environment. To re-create the marking sets, use the appropriate FileNet P8 tools. When you re-create the properties, you must use the same symbolic name that is used in the source environment.

To migrate the marking sets, use FileNet Deployment Manager to export and import the marking sets but not any property templates, which are created when the solution is deployed by IBM Case Manager.

Related tasks:

"Importing IBM Case Manager assets by using a solution manifest" on page 142

Exporting the security configuration

Security configuration settings are stored in a security configuration package file. You can move the file from one environment to another by using the export and import security configuration wizards in the IBM Case Manager administration client. For example, you can create and check your security configuration in a test environment, run the export security configuration wizard, and then import the security configuration package file into production.

About this task

If you configured security for a solution, export the security configuration package file when you migrate the solution package. When you configure the target environment after you deploy the solution, import the security configuration package file so that the settings can be applied to the deployed solution.

Procedure

To export the security configuration:

1. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   `http://server:port/navigator/?desktop=icmadmin`
   server is the IBM Content Navigator IP address or fully qualified server name.
   port is the IBM Content Navigator port number.
2. In the navigation tree in the left pane, select a design object store and click **Solutions**.
3. On the Solutions page in the right pane, select the solution that is associated with the security configuration to export.
4. Click **Actions** > **Export** > **Security Configuration**.
5. Complete the wizard steps and download the security configuration package file.

Related tasks:

"Importing the security configuration" on page 154

"Configuring security by using the IBM Case Manager administration client wizard" on page 84

Exporting the audit configuration

If you configure auditing for a solution, you can view and analyze the case history for the solution. You can move the audit configuration settings from one environment to another by using the export and import audit configuration wizards in the IBM Case Manager administration client. For example, you can create and check your audit configuration in a test environment, run the export audit configuration wizard, and then import the audit definitions into production.

About this task

If you configured auditing for a solution, export the audit configuration package file when you migrate the solution package. When you configure the target environment after you deploy the solution, import the audit configuration package file so that the settings can be applied to the deployed solution.

Procedure

To export the audit configuration:

1. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   `http://server:port/navigator/?desktop=icmadmin`
   server is the IBM Content Navigator IP address or fully qualified server name.
   port is the IBM Content Navigator port number.
2. In the navigation tree in the left pane, select a design object store and click **Solutions**.
3. On the Solutions page in the right pane, select the solution that is associated with the audit configuration to export.
4. Click **Actions** > **Export** > **Audit Configuration**.
5. Complete the wizard steps and download the audit configuration package file.

Related tasks:

"Importing the audit configuration" on page 155

"Configuring auditing" on page 21

Exporting other FileNet P8 assets

If your solution includes assets that were created with other IBM FileNet P8 tools, you cannot use the IBM Case Manager administration client to migrate the assets.

Before you begin

Read the FileNet P8 documentation about FileNet P8 assets. Be sure that you understand the capabilities, limitations, and caveats of moving assets from one environment to another, so that you can make the necessary adjustments in your source and destination environments before you attempt to deploy.

About this task

If you extend your solution with other FileNet P8 assets, you must migrate the assets to the target domain by using the appropriate migration tool for that asset, such as FileNet Deployment Manager or the Process Configuration console.

Follow these procedures to migrate assets from the development environment target object store to the target environment object store. These assets are not recognized by Case Manager Builder, but your business processes might use these assets.

You can also follow these procedures to move a solution from one development environment to another. For example, if you are a solution provider and you want to move your solution from your development environment to your customer's development environment.

"Using FileNet Deployment Manager to export other FileNet P8 assets" on page 136

"FileNet Deployment Manager include options for assets" on page 137

"Exporting other FileNet P8 assets by using the Process Configuration console" on page 139

Related concepts:

FileNet P8 assets

Deployment overview

Related tasks:

"Migrating the translated user interface elements of your case management application" on page 156

Using FileNet Deployment Manager to export other FileNet P8 assets

Use FileNet Deployment Manager to migrate assets that were created with IBM FileNet P8 tools from the development environment target object store to the target environment object store. These assets are not recognized by Case Manager Builder, but your business processes might use these assets.

About this task

This step is required only if you created additional assets in the development environment target object store by using FileNet P8 tools outside of Case Manager Builder. You can also follow this procedure to move a solution from one development environment to another. For example, complete the procedure if you are a solution provider and you want to move your solution from your development environment to your customer's development environment.

If you extend your solution with non-case management assets, you must migrate the assets to the target domain by using the appropriate migration tool for that asset, such as FileNet Deployment Manager for assets that were added with Workplace XT. The IT admin and the business analyst must track these extended assets and ensure that they are properly managed. For example, form templates and some assets are stored in the target object store. If the test environment is reset in Case Manager Builder, these extended assets are lost. To preserve extended assets that reside in the target object store you must export the assets to a protected location, such as a removable disk, by using FileNet Deployment Manager, and then import the assets after the next iteration of the solution is deployed.

Procedure

To move additional assets to a another development or production target object store:

1. Create a list with the description and location of all additional extended assets that are used in the solution design.
2. See the FileNet Deployment Manager documentation for details on the steps in this procedure.

   Tip: Review these sections:
   - **Deploying IBM FileNet P8 applications** > **Deployment overview**
   - **Deploying IBM FileNet P8 applications** > **FileNet P8 assets**
   - **Deploying IBM FileNet P8 applications** > **Prepare data for deployment** > **How to...** > **Prepare Content Engine data**

- **Deploying IBM FileNet P8 applications** > **Deploy FileNet P8 Platform assets** > **How to...** > **Deploy Content Engine** > **Import converted objects**

3. Create the deploy dataset. FileNet Deployment Manager uses the export manifest file to generate a deploy dataset of exported objects.
4. Create the object store, security principal, and optionally service half maps to capture information from the IBM Case Manager development, or source, environment. Follow all recommendations in the FileNet Deployment Manager documentation, such as making a note of the security principals that are discovered to ensure corresponding administrative groups can be identified in the destination environment.
5. Use FileNet Deployment Manager to create a deploy package. A deploy package is a compressed file of deployable content that can be deployed from FileNet Deployment Manager that is on a different system. When you create a deploy package, you specify its deployable content by selecting a deploy dataset folder that was created by the export procedure in step 3. You also have the option of including the half maps that were created in step 4.

FileNet Deployment Manager include options for assets

The include options in FileNet Deployment Manager specify which related objects and associated metadata are included in the export set for an object. The include options must be set correctly to ensure that the object can be imported into any target environment.

The include options for FileNet Deployment Manager control individual assets or objects. The include options that are specified for an asset are propagated to any related objects that are added to the export data set as a result of the include options settings for the original asset. These include options cascade from one object to the next as the export operation finds associated objects to add to the export data set based on the specified include options.

When you use FileNet Deployment Manager to migrate assets for a solution application, specify include options that narrowly target the assets to export. This narrow focus is intended to avoid implicit inclusion of unwanted objects that can be caused by propagation of the include options. In the Include Options window in FileNet Deployment Manager, click **None** to clear all the include options that are selected. After you clear the include options, only the asset that is listed in the export manifest will be exported and placed into the deploy dataset.

In certain cases, such as in the following cases, this narrow focus might need to be broadened:

Objects that are exported along with associated custom metadata

For an object such as a folder or document that is exported with associated custom metadata, such as property templates that are used as metadata to describe custom properties for the folder or document, keep the include options that are selected by default in the **Data Design** section.

Tips:

- For associated metadata that was created in the source system after an add-on was installed, install the same add-on into the target object store instead of moving the metadata by using FileNet Deployment Manager.
- To avoid the accidental inclusion of metadata that is created by the IBM Case Manager deploy solution process, explicitly include any custom metadata in the export manifest instead of implicitly including the metadata by using the **Data Design** include options.

Moving all content in a folder

If all content in a folder is to be moved, export the folder and implicitly include the contents and subfolders with the relationships. In this case, keep the include options that are selected by default in the **Folders and Contained Objects** section.

Tips:

- For more control over the export, add the parent folder explicitly to the export manifest instead of by using the **Include parent folders** option.
- Do not select **Include parent folders** if you export assets in the case instance folder hierarchy. The case folder and case instances must be created by the IBM Case Manager deploy solution process and IBM Case Manager server at runtime.

Associated objects that an asset is dependent on

Explicitly specify in the manifest other associated objects that an asset is dependent on, such as workflow definitions, search templates, and form templates. Select the **Include relationship to containing folders** option and maintain relationships to the parent folder.

Documents that are revised as the solution design changes

For documents that are revised as the solution design changes, such as form templates, search templates, and workflow definitions, use the **Document-Related** > **Include all document versions** include option to ensure that subsequent exports with the same export manifest use the latest of the version document. If you do not want to export all versions, edit the export manifest to delete the document, and then add it to the manifest again to ensure that the export action uses the latest version of the document.

Compound documents, annotations, and thumbnails

Use other document-related include options for compound documents, annotations, and thumbnails on an as needed basis.

Objects with subscriptions and events

For objects with subscriptions and events, implicitly export the subscriptions and events by selecting the **Include event subscriptions attached to objects** and **Include event actions associated with subscriptions** options.

Class definitions

For class definitions, explicitly include the custom property templates and implicitly include the choice lists for the custom property templates. Do not use the **Data Design** include options for the class definitions themselves. This approach reduces potential side-effects that can be caused by the export of property templates from add-ons, or by the export of a case type class definition when an exported object refers to metadata that is associated with the case type, such as a case property or case task. Typically, the **Include modified system classes** option is not selected and should be used with caution.

The **General** include options can typically be left with their default values.

For more information about FileNet Deployment Manager include options, see the IBM FileNet P8 documentation.

Related tasks:

Specify the include options of an asset

Exporting other FileNet P8 assets by using the Process Configuration console

Use the Process Configuration console from within IBM Administration Console for Content Platform Engine to export Process Services assets from the development environment target object store to the test or production environment target object store.

About this task

Export the required Content Platform Engine Process Services assets from the target object store in the project area of the development environment where the solution application was created and tested. Required Process Services assets are assets that are created with the Process Configuration console or Process Designer, not assets that are created in Case Manager Builder.

These assets are not managed by IBM Case Manager, but the solution might incorporate them or the business processes that are part of your solution application might use them. Examples of these assets might be component queues or workflow system configuration parameters.

Procedure

To export other FileNet P8 assets by using the Process Configuration console:

1. In IBM Administration Console for Content Platform Engine, select the target object store and click **Administrative** > **Workflow System**.
2. On the Workflow System tab, click **Actions** > **Configure Workflow Settings**.
3. From the **Workflow Systems** list, select the connection point for the project area where the solution application resides. In the **Action** menu, click **Connect** to log on to the workflow system.
4. In the **Action** menu, click **Export to XML file** to start the export wizard.
5. Complete the steps in the wizard. Keep in mind the following export guidelines:
   - Select only assets that were created with tools other than Case Manager Builder. Migrating assets such as work queues or event logs, which are created by the deploy solution operation, can cause conflicts. Such assets can often be recognized by the presence of the solution prefix in their name or when the asset name is the same as the solution name.
   - Select the **Include System Properties** check box to export workflow system configuration information. Some configuration information is environment-specific. You might need to edit this information by using Process Configuration console on the destination system after the solution application is deployed.
   - If you want to export only system properties, select **Export selected components** under **Export Type**. On the Select Export Components page, clear the check boxes for all components.

What to do next

Include the resulting XML file as a part of the solution application files when you prepare to migrate the solution.

Exporting other IBM and external assets

If your solution includes assets that were created with other IBM products or tools, or with non-IBM products or tools, you cannot use the IBM Case Manager administration client to migrate the assets.

About this task

When you migrate a solution application, you must migrate these extra assets and components to the new environment. The other IBM and external items each have their own tools and procedures for migration, both automated and manual. The team responsible for deploying the solution must work with each of the development teams to determine the appropriate method and order for migrating and deploying these assets.

Example migration models for other types of assets can include:

- Export/Import
- Compile/Install
- Migrate/Deploy
- Delivery of third-party component
- Access to external service

See related topics for information about migrating some of these IBM and external assets.

Related tasks:

Maintaining solutions that are associated with IBM Business Process Manager process applications

Importing IBM Case Manager assets

You use the IBM Case Manager administration client to import a solution from one environment to another.

Before you begin

You must make the solution files available to the IBM Case Manager administration client. Typically, you make the files available by using the administration client to export from solution assets from the design object store. This export process creates a solution package that contains all assets that were created for the solution in Case Manager Builder.

Alternatively, if you are using a version control system (VCS), you can extract the solution files and solution manifest from the VCS to a directory that is accessible to the administration client.

"Importing IBM Case Manager assets by using a solution package"

"Importing IBM Case Manager assets by using a solution manifest" on page 142

Importing IBM Case Manager assets by using a solution package

Use the IBM Case Manager administration client to import a solution package from one environment to another. The solution package that you import includes all assets that were created for the solution in Case Manager Builder.

Procedure

To import a solution package:

1. Copy the compressed file that contains the exported solution package to a location that is accessible by the IBM Case Manager administration client.
2. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   `http://server:port/navigator/?desktop=icmadmin`
   server is the IBM Content Navigator IP address or fully qualified server name.
   port is the IBM Content Navigator port number.
3. In the navigation tree in the left pane, select the design or staging object store to which you want to import the solution and click **Solutions**.
4. On the Solutions page in the right pane, click **Import** > **Import Solution** > **From Solution Package** and complete the wizard steps.

   Tip: By default, the Import Solution wizard is configured to display the target principal mapping step to users. You can hide the target principal mapping from users by clearing the **Enable target principal mapping when importing assets** check box in the wizard.

What to do next

Before you deploy and configure the solution, back up the target environment.

"Reimport of assets with content containing environment-specific references"

Reimport of assets with content containing environment-specific references:

When a solution is reimported to the same object store, environment-specific changes to the assets of that solution might not show up in the reimported version.

When you import a solution package by using the IBM Case Manager administration client or the IBM Case Manager configuration tool, environment-specific values can be mapped from those in the development environment to those in the target environment.

Important: Environment-specific mapping options are not presented when a solution is imported by using a solution manifest file.
If the current version of a solution is reimported into the same design or staging object store multiple times without changes to the solution package, values assigned on the mapping dialogs in the Import Solution Package wizard might not appear in the target system. This can occur when a document object with content is reimported to a destination object store that contains a document object with the same ID.

In IBM FileNet Content Manager, a document object's properties can be modified with a reimport, but the content elements cannot. Solution application artifacts, such as pages that include a website widget or workflow definitions that include URL references, might be affected. Similarly, if non-IBM Case Manager assets that are represented as documents with content are reimported into the same object store multiple times by using FileNet Deployment Manager, modifications to environment-specific information by the FileNet Deployment Manager data conversion feature might not appear in the target system. This can occur with solution application artifacts such as form templates and workflow definitions that include URL references.

If a reimport appears not to convert document content as expected, do one of the following actions:

- From the destination design object store, staging object store, or target object store, delete the current version of the document prior to the reimport. Deleting this version causes the document version to be created, rather than modified, by the reimport.
- If the current document version cannot be deleted prior to the reimport, modify the content manually by using the appropriate tools in the destination object store after the reimport completes.

To find the current version of a document, use the IBM Administration Console for Content Platform Engine to navigate to the destination object store and browse to find the solution folder or the folder that contains the asset. Locate the desired document and use the versions tab on its details pane to view the versions.

Importing IBM Case Manager assets by using a solution manifest

If IBM Case Manager is integrated with a version control system (VCS), you can import solution assets that were exported from the VCS.

About this task

To import a solution from a VCS, you must first export the solution files and solution manifest from the VCS. During the import, you are prompted for the server directory that contains the exported assets and manifest.

Procedure

To import a solution by using a solution manifest:

1. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   `http://server:port/navigator/?desktop=icmadmin`
   server is the IBM Content Navigator IP address or fully qualified server name.
   port is the IBM Content Navigator port number.
2. In the navigation tree in the left pane, select the design or staging object store to which you want to import the solution and click **Solutions**.
3. On the Solutions page in the right pane, click **Import** > **Import Solution** > **From Solution Manifest** and complete the wizard steps.

What to do next

Before you deploy and configure the solution, back up the target environment.

Related tasks:

"Exporting IBM Case Manager assets from a VCS" on page 133

Deploying migrated solutions

Deploying a solution makes it available as an application in the target environment.

About this task

To deploy a solution, you must first deploy any IBM external assets that were created outside of IBM Case Manager and IBM FileNet P8 tools. You then import FileNet P8 assets that must be deployed before the solution package is deployed.

After you deploy the solution with IBM Case Manager, other assets that are managed by FileNet P8 must be deployed.

When you design and create a solution, you must decide what the solution locale is. The solution locale refers to the locale of display names, such as case properties, case types, tasks, and other solution artifacts that you create with Case Manager Builder. When you deploy the solution to a target environment for the first time, you must deploy the solution under the same locale to ensure that the display names are preserved.

"Backing up the target environment before deploying solutions"

"Deploying prerequisite assets"

"Deploying a solution with IBM Case Manager" on page 147

"Deploying postrequisite assets" on page 151

Related concepts:

Prepare data for deployment

Deploy IBM FileNet P8 Platform assets

Backing up the target environment before deploying solutions

Create a backup of the target environment before you deploy any solutions that you migrated.

About this task

For the best possible backup, temporarily suspend, or quiesce, all activity on the system. Quiescing the system allows a consistent snapshot of all related data to be captured. Follow procedures specific to your operating environment to quiesce the system. Ensure, however, that your plan includes how system administrators and solution administrators can access the system to perform the necessary solution deployment and system configuration tasks.

After the backup, minimize access to the system to avoid changes that might make the system inconsistent with the backup. You can resume regular operations after the solution application is fully migrated and deployed.

For details on backups, see the related topic about backing up your IBM Case Manager system.

Related tasks:

"Backing up your system" on page 68

Deploying prerequisite assets

If you extend your solution with non-case management assets, you must migrate the assets to the target domain by using the appropriate migration tool for that asset, such as FileNet Deployment Manager for assets managed by the Content Platform Engine or the Process Configuration console for Content Platform Engine Process Services objects. Some assets must be deployed before you use the IBM Case Manager administration client to deploy the solution package.

About this task

This task is required only if you created additional assets in the development environment target object store by using IBM FileNet P8 tools outside of Case

Manager Builder. Importing the following types of assets also deploys the assets. The assets become operational in the target environment after you import them.

- Content Platform Engine Content Services assets that the solution depends on, such as reused property templates, document classes, or choice value lists. If the target environment already contains the reused metadata, this step is not required.
- Content Platform Engine Process Services assets that are incorporated into the solution, such as a workflow system configuration or component queues.
- Artifacts that were created with other IBM or external tools outside of IBM Case Manager and FileNet P8 tools.
- Widgets that must be registered before the solution package is deployed.

"Importing assets by using FileNet Deployment Manager"

"Importing assets by using the Process Configuration console" on page 146

Related concepts:

Prepare data for deployment

Deploy IBM FileNet P8 Platform assets

Importing assets by using FileNet Deployment Manager

Other IBM FileNet P8 assets in the solution application that are managed by the Content Platform Engine are converted, analyzed, and imported by using the FileNet Deployment Manager.

About this task

The solution administrator and business analyst must track these extended assets and ensure that they are properly managed. For examples and more details, see the topics about identifying solution assets for migration.

Procedure

To deploy additional Content Platform Engine assets to another development or production target object store, use FileNet Deployment Manager:

1. Place the exported deploy dataset onto a system where the FileNet Deployment Manager tool is installed and has access to the target environment. The exported data is typically transferred as a compressed file, such as a ZIP file. Expand the compressed file into a deploy dataset folder of a FileNet Deployment Manager deployment tree.

   If the data was transferred as a FileNet Deployment Manager Deploy Package, use the FileNet Deployment Manager **Expand Deploy Package** operation to expand the compressed file. The extraction places the data into the selected deploy dataset folder. You can also choose to extract the halfmaps into a source environment that exists in FileNet Deployment Manager.

   If the data is not a Deploy Package, the halfmaps for both the source and destination environments must be available to the FileNet Deployment Manager instance that performs the import. These halfmaps can either be created, if the source environment is available, or passed along with the deploy dataset. The preferred method for this second option is to use a Deploy Package.
2. Populate the halfmaps for the destination environment.
3. Join the source and destination halfmaps to create data maps by associating correct mappings for object stores, security principals, and services between the environments. Follow all recommendations in the FileNet Deployment Manager

documentation. For example, ensure that there are corresponding administrative groups in the source and destination environments with privileges appropriate for importing and deploying the solution application. The security principal mapping must also consider the ownership of assets, as described in the summary of key options in step 6.

4. Convert the objects in the deploy dataset for import. FileNet Deployment Manager creates the converted data set into a new subfolder of the folder that you specified. The subfolder is named after the deploy dataset name with `.converted` appended to the name.
5. Generate and review the analysis of the impact report to verify the effect that the import operation has on the target environment. The change impact analysis operation also validates the converted deploy dataset file with the destination environment. This operation provides information only; it does not actually import data or modify the destination environment in any way.
6. Import the converted deploy dataset. Keep in mind the following import guidelines:
   - Some assets in the target object store are required by the solution deployment and must be imported as prerequisite assets. Some assets depend on the solution being deployed before they can be successfully imported and must be imported as postrequisite assets. However, some assets can be imported either before or after the solution is deployed if the validation logic in the solution deployment or the import operation do not enforce the presence of the asset or its dependents for a successful deployment. Those assets can be packaged with either the prerequisite or postrequisite assets. To avoid potential issues, consider how the asset is used in the solution and choose a package that makes the most sense for the overall solution application deployment process.
   - Deploy metadata extensions that were created by using the Content Platform Engine addOns feature to the non-development target object store. Deploy these extensions by using the same methods that were used when the asset was originally added to the development environment target object store. For example, install the integrated product into the non-development environment and apply the addOn to the target object store, as directed by the product documentation.
   - Summary of key import options:

     Import Owner
     Ownership of solution application assets in the target environment must be included in the security planning for the solution. Choose this option to retain the owner information from the source environment. Use data mapping for the security principals if you plan to switch ownership to another user in the destination environment.

     Import Object ID
     This option must be selected.

     Use Original Create/Update Timestamps and Users
     Select this option only if the **Update if Newer** option is also selected. Selecting this option might cause modifications to Content Platform Engine system properties. To modify system properties, the FileNet P8 domain user that is logged in to FileNet Deployment Manager must have the **Modify certain system properties** privilege on the destination object store or the import operation returns errors.

Transfer workflows after import
Select this option if the import includes a workflow definition document that is to be used as the current version in the destination environment, and you want FileNet Deployment Manager to automatically transfer the workflow definition into the destination workflow system as a part of the import process. If the workflow definition references a Content Platform Engine Process Services asset like a component queue, the import or definition of that component queue must be performed first.

Always Update vs. Update if newer
Because it is important for a solution application deployment to fully replicate the design from the source development environment, use of the **Always Update** option is typical. However, if your business needs require that assets modified directly in the target environment take precedence over older changes from the IBM Case Manager development environment, you can select the **Update if newer** option. The DateLastModified property on the objects in the deploy dataset are compared to the same objects in the target environment to determine which objects are newer.

Related concepts:

Prepare data for deployment

Deploy IBM FileNet P8 Platform assets

Related tasks:

"Identifying solution assets for migration" on page 117

Importing assets by using the Process Configuration console

Import the required Content Platform Engine Process Services assets into the target environment where the solution application is to be deployed. Required Process Services assets are assets that are created with the Process Configuration console or Process Designer, not assets that are created in Case Manager Builder.

About this task

These assets are not managed by IBM Case Manager, but the solution might incorporate them or the business processes that are part of your solution application might use them. Examples of these assets might be component queues or workflow system configuration parameters.

Procedure

Use the Process Configuration console from within IBM Administration Console for Content Platform Engine to import Process Services assets from the development environment target object store to the test or production environment target object store:

1. Start the Process Configuration console. For an object store on the Administrative node, click **Workflow System** > **Actions** > **Configure Workflow Settings**.
2. From the **Workflow Systems** list, select the connection point for the project area where the solution application is to be deployed. In the **Action** menu, click **Connect** to log on to the workflow system.
3. In the **Action** menu, click **Import to XML file** to start the import wizard.
4. Complete the steps in the wizard. Keep in mind the following import guidelines:

- Use the **overwrite** option to add new objects or properties or to replace existing objects or properties in the destination isolated region. If any transferred workflows use a queue, the queue is overwritten even if the workflows are not running at the time of the import. If the overwrite attempts to remove items that are referenced, such as exposed fields or operation parameters, then the import will fail (referenced items cannot be removed).
- Use the **merge** option to add objects or properties to the destination isolated region if these objects or properties do not exist in the destination isolated region. If the destination isolated region contains objects or properties with the same name as those in the source isolated region, the items are merged. Thus, for a solution redeployment, the **merge** option preserves any existing properties in the destination target environment and adds new properties from the development environment project area. Use of the **merge** option is typical.
- If the exported source contains system properties, the import operation skips the import of user information if the user is not defined on the destination system. This operation applies to both overwrite and merge. You can use FileNet Deployment Manager to prepare the data for deployment by mapping user information to values appropriate for the destination target environment.

Related concepts:

Prepare data for deployment

Deploy IBM FileNet P8 Platform assets

Related tasks:

"Identifying solution assets for migration" on page 117

Deploying a solution with IBM Case Manager

When you deploy a solution to a target object store, the items that are defined in the solution package are created in the target object store. For example, the document types that you defined are created as document class instances.

Before you begin

Ensure that you exported the solution package from the development environment design object store and imported it to the staging object store.

Be sure to have your completed configuration checklist available.

Procedure

To deploy a solution:

1. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   `http://server:port/navigator/?desktop=icmadmin`
   server is the IBM Content Navigator IP address or fully qualified server name.
   port is the IBM Content Navigator port number.
2. In the navigation tree in the left pane, select a design object store and click **Solutions**.
3. On the Solutions page in the right pane, select the solution that you want to deploy.
4. Click **Actions** > **Deploy** and complete the wizard steps.

You can deploy a solution from either a development environment design object store or a production environment staging object store. If you deploy from a development environment design object store, the target environment name field is automatically populated by the wizard. If you deploy from a production environment staging object store, you must select the target environment name from the **Target Environments** list. This list contains the target environments in the production environment staging object store that have the same integration type as the solution.

Tip: If you do not perform certain prerequisite steps, the solution deployment might succeed with warning messages. Review the deployment log to determine if additional actions are required.

5. Optional: After the solution is deployed, assign users to the roles for this case:
   a. Click **Assign Roles**. The Case Manager Client opens for you to assign users to the roles for this solution.
   b. Add users to the roles.

      Tip: You can add users later by using Case Manager Client.
   c. Click **View Log** to download and view the solution deployment log.

Related tasks:

Configuration checklist

Configuring the production environment

Configuring the production environment

Deploying a solution to a production target object store by using the command line

When you deploy a solution to a production target object store, the items that are defined in the solution package are created in the target object store. For example, the document types that you defined are created as document class instances.

Before you begin

Ensure that you exported the solution package from the development environment design object store and imported it to the production environment staging object store.

Be sure to have your completed configuration checklists available.

About this task

The administration client stores your settings for the case deployment profile in a set of XML configuration files that is called a profile. The XML files contain the properties and values that describe the associated configuration and deployment tasks. You must provide values for the profile properties that are specific to each configuration at your site, such as the application server name.

The following table lists the configuration information and the file for deploying a solution to a production object store.

Table 17. Case deployment configuration tasks and files

Configuration and task information	XML file
Settings for deploying an IBM Case Manager solution into a production target object store. You need one configuration file for each production environment target object store that you deploy a solution to. You can create additional task files in the same profile, or you can create a separate profile for the additional settings. When you generate a second solution deployment configuration file in a profile, it is named `deploysolution.2.xml`. The file name increments for each new file that you generate. You cannot change the file name, but you can edit the value in the file for the name of the task.	`deploysolution.xml` `deploysolution.`*n*`.xml`. *n* is an integer starting with 2.

Procedure

To deploy a solution:

1. Change the current directory to the *install_path*`/CaseManagement/configure` directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the `/opt/IBM/CaseManagement` directory.
Windows	By default, *install_path* is the `C:\Program Files\IBM\CaseManagement` directory for a fresh install or the `C:\Program Files (x86)\IBM\CaseManagement` directory for an upgrade.

2. If you want to create additional deployment configuration files in the same profile, generate an additional `deploysolution.`*n*`.xml` file by running the following command. Do not type any line breaks when you enter the command:

```
configmgr_cl generateConfig
 -task deploysolution
 -profile myprofile
 -profileType profileType
 [-silent] [-force]
```

-profile *myprofile*

Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*`/CaseManagement/configure/profiles` directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1"` or `/opt/IBM/CaseManagement/configure/profiles/develop1`.

- The full path to the profile input file, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp"` or `/opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp`.

-profileType *profile_type*
Specifies the type of profile and must be `wasproductionenvironment` for WebSphere Application Server or `wlproductionenvironment` for Oracle WebLogic Server.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

For example, the following command generates one `deploysolution.n.xml` files for the existing case deployment profile that is named deploy_solution:

```
configmgr_cl generateConfig
 -task deploysolution
 -profile deploy_solution
```

3. Edit the property values in the `deploysolution.xml` files that you generated in the case deployment profile:
   a. Use a text editor or XML editor to open one of the configuration XML files that you generated.
   b. Replace each occurrence of `****INSERT VALUE****` with a value appropriate for your site. See the descriptions in the file for more information and use your configuration checklists.

      Important: You are not required to store values for passwords in the file. You can run the **storePasswords** command later to add encrypted passwords to the file.
   c. Replace empty values that have the format `<value />` with a value appropriate for your site. Use the format `<value>my_value</value>`.
   d. Verify that the default values for the remaining properties are correct for your site.
   e. Set the **enabled** attribute value in the <configuration> tag to `true` in any configuration XML file that you edit if you want to run the configuration task. When a task is disabled, the **execute** command skips the task.
   f. Save your edits and close the XML file.
   g. Repeat as needed until you edit all the `deploysolution.n.xml` files for your profile.
4. Run the `deploysolution` tasks in the profile one at a time by running the following command. Do not type any line breaks when you enter the command:

```
configmgr_cl execute -taskfile task_file_name
 -profile myprofile [-silent] [-force]
```

Where *task_file_name* is the name of the task file: `deploysolution.xml` or `deploysolution.n.xml` and *n* is a number larger than 2.

5. Repeat 4 on page 150 as needed for each deploy solution task file that you generated in this profile.
6. Optional: Assign users to the roles for this case:
   a. Run the test command to assign users by running the following command. Do not type any line breaks when you enter the command:

      ```
      configmgr_cl test -taskfile task_file_name
       -profile myprofile [-silent][-force][-help]
      ```

      Where *task_file_name* is the name of the task file: `deploysolution.xml` or `deploysolution.n.xml` and *n* is a number larger than 2. The Case Manager Client opens for you to assign users to the roles for this solution.
   b. Add users to the roles.
   c. Repeat as needed for each deploy solution task file that you generated in this profile.

Related reference:

"**test** command" on page 422

"**generateConfig** command" on page 347

Deploying postrequisite assets

Some assets must be deployed after you use the IBM Case Manager administration client to deploy the solution package.

About this task

Importing the following types of assets also deploys the assets. The assets become operational in the target environment after you import them.

- Content Platform Engine Content Services assets that depend on artifacts in the solution, such as a stored search that references case properties and is used with a Content List widget
- IBM Content Navigator desktop and other configuration information that is related to running the solution application
- Artifacts that were created with other IBM or external tools outside of IBM Case Manager and IBM FileNet P8 tools

"Importing assets with FileNet Deployment Manager after solution deployment"

Importing assets with FileNet Deployment Manager after solution deployment

Depending on the solution assets, you might need to use FileNet Deployment Manager to import some assets after the solution is deployed, such as Content Platform Engine Content Services assets that depend on artifacts in the solution.

About this task

The solution administrator and business analyst must track these extended assets and ensure that they are properly managed. For examples and more details, see the topics about identifying solution assets for migration.

Procedure

To deploy additional Content Platform Engine assets to another development or production target object store, use FileNet Deployment Manager:

1. Place the exported deploy dataset onto a system where the FileNet Deployment Manager tool is installed and has access to the target environment. The exported data is typically transferred as a compressed file, such as a ZIP file. Expand the compressed file into a deploy dataset folder of a FileNet Deployment Manager deployment tree.

   If the data was transferred as a FileNet Deployment Manager Deploy Package, use the FileNet Deployment Manager **Expand Deploy Package** operation to expand the compressed file. The extraction places the data into the selected deploy dataset folder. You can also choose to extract the halfmaps into a source environment that exists in FileNet Deployment Manager.

   If the data is not a Deploy Package, the halfmaps for both the source and destination environments must be available to the FileNet Deployment Manager instance that performs the import. These halfmaps can either be created, if the source environment is available, or passed along with the deploy dataset. The preferred method for this second option is to use a Deploy Package.
2. Populate the halfmaps for the destination environment.
3. Join the source and destination halfmaps to create data maps by associating correct mappings for object stores, security principals, and services between the environments. Follow all recommendations in the FileNet Deployment Manager documentation. For example, ensure that there are corresponding administrative groups in the source and destination environments with privileges appropriate for importing and deploying the solution application. The security principal mapping must also consider the ownership of assets, as described in the summary of key options in step 6.
4. Convert the objects in the deploy dataset for import. FileNet Deployment Manager creates the converted data set into a new subfolder of the folder that you specified. The subfolder is named after the deploy dataset name with `.converted` appended to the name.
5. Generate and review the analysis of the impact report to verify the effect that the import operation has on the target environment. The change impact analysis operation also validates the converted deploy dataset file with the destination environment. This operation provides information only; it does not actually import data or modify the destination environment in any way.
6. Import the converted deploy dataset. Keep in mind the following import guidelines:
   - Some assets in the target object store are required by the solution deployment and must be imported as prerequisite assets. Some assets depend on the solution being deployed before they can be successfully imported and must be imported as postrequisite assets. However, some assets can be imported either before or after the solution is deployed if the validation logic in the solution deployment or the import operation do not enforce the presence of the asset or its dependents for a successful deployment. Those assets can be packaged with either the prerequisite or postrequisite assets. To avoid potential issues, consider how the asset is used in the solution and choose a package that makes the most sense for the overall solution application deployment process.
   - Deploy metadata extensions that were created by using the Content Platform Engine addOns feature to the non-development target object store. Deploy

these extensions by using the same methods that were used when the asset was originally added to the development environment target object store. For example, install the integrated product into the non-development environment and apply the addOn to the target object store, as directed by the product documentation.

- Summary of key import options:

  Import Owner
  Ownership of solution application assets in the target environment must be included in the security planning for the solution. Choose this option to retain the owner information from the source environment. Use data mapping for the security principals if you plan to switch ownership to another user in the destination environment.

  Import Object ID
  This option must be selected.

  Use Original Create/Update Timestamps and Users
  Select this option only if the **Update if Newer** option is also selected. Selecting this option might cause modifications to Content Platform Engine system properties. To modify system properties, the FileNet P8 domain user that is logged in to FileNet Deployment Manager must have the **Modify certain system properties** privilege on the destination object store or the import operation returns errors.

  Transfer workflows after import
  Select this option if the import includes a workflow definition document that is to be used as the current version in the destination environment, and you want FileNet Deployment Manager to automatically transfer the workflow definition into the destination workflow system as a part of the import process. If the workflow definition references a Content Platform Engine Process Services asset like a component queue, the import or definition of that component queue must be performed first.

  Always Update vs. Update if newer
  Because it is important for a solution application deployment to fully replicate the design from the source development environment, use of the **Always Update** option is typical. However, if your business needs require that assets modified directly in the target environment take precedence over older changes from the IBM Case Manager development environment, you can select the **Update if newer** option. The DateLastModified property on the objects in the deploy dataset are compared to the same objects in the target environment to determine which objects are newer.

Configuring the target environment after solution deployment

After you migrate a solution and deploy the solution package and its related assets, you must configure some system settings to make the solution operational.

About this task

You must configure security settings and audit definitions. If applicable in your application, you must migrate any translated user interface elements. You must also repeat some system configuration settings each time that you deploy the solution.

Consult your customized migration and deployment instructions for information about configuration settings for your system.

"Importing the security configuration"

"Importing the audit configuration" on page 155

"Migrating the translated user interface elements of your case management application" on page 156

"Configuring system settings after solution deployment" on page 159

"Opening a specific solution page" on page 160

Related tasks:

"Setting up target environments" on page 54

Importing the security configuration

If you exported the security configuration package file for a solution when you migrated the solution package, import the file after you deploy the solution in the target environment to apply the security settings to the solution.

About this task

As discussed in "Configuring security by using the IBM Case Manager administration client wizard" on page 84, the design of a solution includes implementing a security configuration to ensure that cases and case documents are visible and editable only by authorized users and groups. The security configuration can be defined in several ways:

- The security configuration might be defined entirely by using the IBM Case Manager administration client to create a security configuration package.
- The security configuration might be partially defined by using the administration client and partially defined by applying manual steps.
- The security configuration might be entirely defined by manual steps without using the administration client.

When a solution is deployed into a test or production environment, the business analyst or solution developer often assists with designing the security configuration for the test or production environment. For assistance with configuring security, the solution administrator can also consult the customized migration and deployment instructions that were developed for migrating the solution application package.

If the IBM Case Manager administration client was used to implement the security configuration design, security configuration settings are stored in a security configuration package file. You can move this file from one environment to another by using the export and import security configuration wizards in the IBM Case Manager administration client. For example, you can create and check your security configuration in a test environment, run the export security configuration wizard, and then import the security configuration package file into production.

If you manually set up the security configuration for the solution, then you must manually reapply the security configuration in the target environment. You cannot use this procedure to import and apply the security configuration.

Procedure

To import the security configuration package file:

1. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   `http://server:port/navigator/?desktop=icmadmin`
   server is the IBM Content Navigator IP address or fully qualified server name.
   port is the IBM Content Navigator port number.
2. In the navigation tree in the left pane, select a design object store and click **Solutions**.
3. On the Solutions page, click **Actions** > **Import** > **Security Configuration**, browse to the exported security configuration package file, and complete the wizard steps.
4. After you import the file, view the security configuration to ensure that it is correct for the target environment.
5. Apply the security configuration to the deployed solution.

Related concepts:

"Older versions of an audit or security configuration in the IBM Case Manager administration client might not be re-imported" on page 204

Related tasks:

"Preparing customized migration and deployment instructions" on page 127

"Exporting the security configuration" on page 134

"Configuring security by using the IBM Case Manager administration client wizard" on page 84

Importing the audit configuration

If you exported the audit configuration package file for a solution when you migrated the solution package, import the file after you deploy the solution in the target environment to apply the audit settings to the solution.

About this task

As discussed in "Configuring auditing" on page 21, the design of a solution includes implementing auditing to track the history of cases. The audit configuration can be defined in several ways:

- The audit configuration might be defined entirely by using the IBM Case Manager administration client to create an audit configuration package.
- The audit configuration might be partially defined by using the administration client and partially defined by applying manual steps. For example, configuring the audited properties by using the IBM Case Manager administration client is sufficient for support of the Timeline Visualizer widget to view case history. But integration with the IBM case analytics tools typically requires additional, manual steps.
- The audit configuration might be entirely defined by manual steps without using the administration client.

When a solution is deployed into a test or production environment, the business analyst or solution developer often assists with designing the audit configuration for the test or production environment. For assistance with configuring auditing, the solution administrator can also consult the customized migration and deployment instructions that were developed for migrating the solution application package.

If the IBM Case Manager administration client was used to implement the audit configuration design, audit configuration settings are stored in an audit

configuration package file. You can move this file from one environment to another by using the export and import audit configuration wizards in the IBM Case Manager administration client. For example, you can create and check your audit configuration in a test environment, run the export audit configuration wizard, and then import the audit configuration package file into production.

If you manually set up audit definitions for a solution to support IBM Case Manager history and analytics extensions, then you must manually reconfigure the audit definitions in the target environment. You cannot use this procedure to import the audit configuration. For information, see IBM Case Manager history and analytics extensions.IBM Case Manager history and analytics extensions..

Procedure

To import the audit configuration:

1. Start the IBM Case Manager administration client. Enter the following URL in a browser:
   `http://server:port/navigator/?desktop=icmadmin`
   server is the IBM Content Navigator IP address or fully qualified server name.
   port is the IBM Content Navigator port number.
2. In the navigation tree in the left pane, select a design object store and click **Solutions**.
3. On the Solutions page, click **Actions** > **Import** > **Audit Configuration**, browse to the exported audit configuration package file, and complete the wizard steps.
4. After you import the file, view the audit configuration to ensure that it is correct for the target environment.
5. Apply the audit configuration to the deployed solution.

Related concepts:

"Older versions of an audit or security configuration in the IBM Case Manager administration client might not be re-imported" on page 204

Related tasks:

"Preparing customized migration and deployment instructions" on page 127

"Exporting the audit configuration" on page 134

"Configuring auditing" on page 21

"Preparing a database for the case history store" on page 61

Migrating the translated user interface elements of your case management application

You can migrate the translated user interface in your case management application by exporting translated artifacts from the source domain and deploying them in the target domain.

Procedure

To migrate the translated user interface elements of your case management application to another target environment, complete the following steps:

1. Export or generate versions of the translated solution artifacts:

Option	Description
Content-related artifacts: Property templates, choice lists, document types, case types, and tasks	Use IBM FileNet Deployment Manager to export the translated assets that are managed by the Content Platform Engine in the target object store: 1. Create an export manifest and add property templates, choice lists, and class definitions, including case types and document types and tasks. Set the Include Options to none. 2. Export the assets. 3. Create a compressed file to use as a deployment package. Be aware of the following situations: • If your solution exposes all of the document types in the target object store in case client, you must translate all document types. If your solution is configured to expose only the document types that are defined in your solution, then translate only those document types. • You need to translate only discretionary tasks. Automatic or manual tasks do not use translated names at run time by design.
Form templates and localization proxy document	Use IBM FileNet Deployment Manager to export translated assets that are managed by the Content Platform Engine in the target object store: 1. Create an export manifest with the translated form template documents and localization proxy document. 2. Export the assets. **Tip:** If the translated assets exist in the same object store folder as the originals, you can export the entire folder. Use the IBM FileNet Deployment Manager **Include Options** to include all of the folder contents. If you want to manage the translated forms separately from the originals, then create a separate export manifest for the translated forms. 3. Create a compressed file to use as a deployment package.
Process-related artifacts	Create a compressed file that contains the `PEAuthoredNames.jar` file, which is in the *`ICN_install_path`*`\ECMClient\configure\explodedformat\navigator\WEB-INF\lib` folder.
Page and view artifacts	Translated pages and view resources are included in the solution package when you export the solution.

2. By using the IBM Administration Console for Content Platform Engine, browse to the *`design_object_store`*`/IBM Case Manager/Solutions/`*`solution_name`* folder.
   a. Create a subfolder of any valid name in this folder, such as `NonICMAssets`, if the subfolder does not exist.
   b. Add all of the compressed files that contain the exported translations to the *`design_object_store`*`/IBM Case Manager/Solutions/`*`solution_name`*`/NonICMAssets` folder in the source environment design object store. Add each compressed file as a separate document object and check in as major version.

3. By using the IBM Case Manager administration client, export your solution from the source domain. The compressed files that contain the translations are checked into the solution folder, so the exported solution package contains the translations.
4. Using the IBM Case Manager administration client, import your solution into the target domain.
5. Deploy the solution to the target environment in the target domain.

   When you design and create a solution, you must decide what the solution locale is. The solution locale refers to the locale of display names, such as case properties, case types, tasks, and other solution artifacts that you create with Case Manager Builder. When you deploy the solution to a target environment for the first time, you must deploy the solution under the same locale to ensure that the display names are preserved.

   If you use Case Manager Builder to deploy the solution, change the browser locale.

   If you use the administration client to deploy the solution, change the browser locale or change the application language value in the Change Language and Locale Settings window.

   If you use the configuration tool to deploy the solution, change the JVM locale in which the configuration tool runs. Edit the `configmgr.ini` or `configmgr_cl.ini` file in the *`ICM_install_dir`*`\configure` folder and change the **`nl`** value to specify your language locale. The default value is en_US.
6. Deploy any assets that are not part of IBM Case Manager into the target domain that is used by your solution. If a single deployment package contains the original and translated form templates and localization proxy document, deploying these other assets also deploys those translated form assets.
7. By using the IBM Administration Console for Content Platform Engine, browse to the `IBM Case Manager/Solutions/`*`solution_name`*`/NonICMAssets` folder in the design object store in the target domain. Download the translated artifacts.
8. Deploy the translated artifacts of your solution to the target domain.

Option	Description
Content-related artifacts: Property templates, choice lists, document types, case types, and tasks	Use IBM FileNet Deployment Manager to import the deployed data set that contains the property templates, choice lists, and class definitions. Import into the target object store that the solution was deployed to. In the import wizard, choose following import options: • Standard Options: Select Import Object ID, leave all other options unselected • Update Options: Update if newer or Always update • Create Options: Never create • Property Update Options: Update only localized properties for class definitions, property templates, and choice lists
Form templates and localization proxy document	Use IBM FileNet Deployment Manager to import the translated form templates and localization proxy document into the target object store that the solution was deployed to. If the deployment package also contains the original form templates, you can skip this step. The previous step of deploying non-IBM Case Manager assets also deployed the translated form templates and localization proxy document

Option	Description
Process-related artifacts	1. Extract the compressed file that contains the `PEAuthoredNames.jar` file. 2. Open the `PEAuthoredNames.jar` file to retrieve the XLIFF files. 3. Rename the `PEAuthoredNames_`*`sourcePERegionID_lang`*`.xliff` file to `PEAuthoredNames_`*`targetPERegionID_lang`*`.xliff`. *PERegionID* is the region ID of the Content Platform Engine, which you can find by using the process configuration console, and *lang* is the two letter language code. 4. Repackage the `PEAuthoredNames.jar` file: a. Create a staging directory. For example,`C:\temp`. b. Create the destination directory for the XLIFF files in the staging directory. For example, `C:\temp\XLIFF`. c. From the destination directory, create the `PEAuthoredNames.jar` file. For example, **jar -cvf PEAuthoredNames.jar *.xliff** 5. Add the `PEAuthoredNames.jar` to the *`ICN_install_path`*`\ECMClient\configure\explodedformat\navigator\WEB-INF\lib` folder. 6. Run the Build the Web Application task and Deploy the Web Application task from the IBM Content Navigator configuration and deployment tool.
Page and view artifacts	Translated pages and view resources are included in the exported solution package. They are deployed to the target environment by deploying the solution.

9. Restart the web application server in which IBM Case Manager is deployed in your target domain, and then redeploy your solution.

Related tasks:

"Migrating solutions" on page 131

"Exporting other FileNet P8 assets" on page 135

"Translating your case management application" on page 37

Configuring system settings after solution deployment

Some system configuration settings, such as those required to support any external assets that you migrated and deployed, must be reconfigured each time that you deploy or redeploy the solution.

About this task

Consult your customized migration and deployment plan for information about required system configuration. Changes that you must apply depend on the assets that are deployed to support your solution.

Related tasks:

"Preparing customized migration and deployment instructions" on page 127

Opening a specific solution page

You can create a URL that opens a specific page of a solution after users log on to Case Manager Client.

About this task

The URL can open a solution page that was created in Case Manager Builder in the **Solution Pages** section of **Pages** tab. The URL can open only a static solution page that can be assigned to a role. The URL cannot open a dynamic solution page, such as a page that was created in the **Case Details Pages** section of the **Pages** tab.

The URL has the following format:

http://*server_name*:*port_number*/navigator/?desktop=icm&feature=Cases &tos=TOS03_ccp00010&solution=*solution_prefix*&page=*page_ID* &pageType=staticPage

`solution_prefix`
The prefix of the solution that you want to open.

`page_ID`
A unique identifier for the static solution page that you want to open.

Procedure

To create a URL that opens a specific solution page:

1. Determine the base URL of a solution by clicking the **Test** link in Case Manager Builder. To find the **Test** link, hover the cursor over the solution on the **Manage Solutions** page.

   For example, the base URL of a solution with a prefix of ABC123 has the following format:

   http://MyServer:Port/navigator/?desktop=icm&feature=Cases &tos=TOS03_ccp00010&solution=ABC123
2. Add the following page information to the base URL: &page=*page_ID* &pageType=staticPage

   To find the page ID, open the solution in Case Manager Builder. The page ID is displayed in the **Unique Identifier** box in the **Solution Pages** section of the **Pages** tab.

   For example, if you want a solution page with the MyWork page ID to open when users log on to Case Manager Client, use the following URL:

   http://MyServer:Port/navigator/?desktop=icm&feature=Cases &tos=TOS03_ccp00010&solution=ABC123&page=MyWork&pageType=staticPage

Modifying solutions after deployment

If you update the solution design, you can redeploy the solution to a production object store that already contains cases for the solution. Modifying a case and redeploying it affects existing case data and new case data. Before you modify a solution that was deployed into production, you must plan for how the changes affect both your new cases and existing cases.

"Redeployment restrictions for modifying a solution" on page 161

"Synchronizing cases with solution data" on page 167

Redeployment restrictions for modifying a solution

You can redeploy a solution to an object store. For example, you can update the solution design and then deploy the solution to a production object store that already contains cases for the solution. Modifying a case and redeploying it affects existing case data and new case data. Before you modify an existing solution, make sure that your changes will not cause problems when you redeploy the solution to an object store that already was associated with that solution.

The following table describes the effects of redeploying a modified solution to an object store.

Table 18. Affects of solution design changes

Type of changes	Result	Comments
New item, such as a new property, a new document type, a new case type, a new task, or a new role	No issues.	
Delete an item, such as a property, a document type, a case type, a task, or a role	No issues.	The item is not removed from the target object store or the Content Platform Engine. Remove any unused roles or in-baskets by using the Process Configuration Console.
Remove a property from a child or parent document type	No issues.	The property is not removed from document type in the target object store or Content Platform Engine. In the development environment, you can edit the document type definition in IBM Administration Console for Content Platform Engine to remove the property.
Adding a property that was previously removed from a child or parent document type to a different document type in the same tree	Not supported.	The change is not replicated correctly in the document type tree in the target object store or Content Platform Engine.
Solution name or prefix	Not supported.	You cannot change the solution name or the solution prefix.
Solution description	No issues.	
Solution icon	No issues.	

Table 18. Affects of solution design changes (continued)

Type of changes	Result	Comments
The property data type, the unique ID (also called symbolic name), or the cardinality for existing properties	Not supported.	Content Platform Engine does not support the following changes to an existing property: • Changing the type of the property, for example, changing from Boolean to String. • Changing the unique ID • Changing a single-value property to a multi-value property or changing a multi-value property to a single-value property If you need to change the data type or cardinality, you must reset the development environment in Case Manager Builder, then change the property in the solution. See the note after this table for more information on the unique ID.
The property name or description	Existing items are affected.	All existing and new instances of a case and document use the updated property name (display name) and description.
The default value for a property	Only new items are affected.	New instances of a case or document that has the property will use the updated default values. Existing instances are unchanged.
The minimum or maximum value for a property	Some existing items are affected.	The existing values are validated against the new minimum or maximum value only when there is an update to the property. New instances are validated against the new minimum or maximum value. Changing the minimum and maximum values can cause a case to have invalid values. The business analyst should manage solution backward compatibility or use the external data service integration to address the change requirements.

Table 18. Affects of solution design changes (continued)

Type of changes	Result	Comments
Choice lists for a property	Existing items are affected.	Changing the choice list values or adding a choice list causes the new values to be displayed as choices. **Note:** It is recommended that you do not remove choice list values because application features can be affected. For example, searching for cases that contain the removed values. The business analyst should manage solution backward compatibility or use the external data service integration to address the change requirements.
Required property setting	Some existing items are affected.	Existing instances require a value for the property only if the instance is updated. New instances require a value for the property. The business analyst should manage solution backward compatibility or use the external data service integration to address the change requirements.
Hidden property setting	Existing items are affected.	All existing instances of the property and new instances use the updated setting. If the property was changed from hidden to visible, then all existing instances and new instances display the property. If the property was changed from visible to hidden, then all existing instances and new instances do not display the property.
Modify a role name in a deployed solution.	When the solution is redeployed, Case Manager Client will display the previous role name and the new role name.	Use Process Configuration Console to remove the unwanted role name.
Modify an in-basket name or hide an in-basket	When the solution is redeployed, Case Manager Client will display the previous in-basket name and the new in-basket name.	Use Process Configuration Console to remove the unwanted in-basket name.
Document type unique ID (also called symbolic name)	Not supported.	Content Platform Engine does not support changing the unique ID.

Table 18. Affects of solution design changes (continued)

Type of changes	Result	Comments
Document type name and description	New and existing items are affected.	New and existing instances use the new display name and description.
Case type unique ID (also called symbolic name)	Not supported.	Content Platform Engine does not support changing the unique ID.
Case type name and description	New and existing items are affected.	New and existing instances use the new display name and description.
Initiating document type for a case type to a different type or to none	New cases are affected.	Existing case instances are not affected because the initiating document type only determines when new cases are created. Only a new instance of a document can start a new case. An existing document cannot start a case.
Case folder structure for a case type	New cases are affected.	New instances of the case use the updated folder structure. In the production environment, your IT administrator can run the case synchronizer utility for existing case instances to add new case subfolders as needed.
Case views	New and existing items are affected.	New and existing case instances use the new view definitions.
New case page or case view page for a case type	Existing cases are affected.	Existing cases and new cases use the updated page definitions.
Task unique ID (also called symbolic name)	Not supported.	Content Platform Engine does not support changing the unique ID.
Task name and description	Only new items are affected.	Only new instances use the new display name. Task instances do not have descriptions.
The criteria changes for a task with a **A property condition is met** precondition The precondition changes from **A document is filed in the case** or **A case property is updated** to **A property condition is met** Or, any precondition changes to **No precondition**	Only new items are affected	You can redeploy the solution, and then ask your IT administrator to run the precondition checker utility to make this change in existing cases.

Table 18. Affects of solution design changes (continued)

Type of changes	Result	Comments
Task precondition, any other change	No issues	If this solution is in development, you can reset the test environment and redeploy.
Task start changed from Manual to Automatic	No issues.	Existing tasks keep the existing Manual setting.
Task start changed from Automatic to Manual	No issues.	Existing tasks keep the existing Automatic setting. New tasks use the Manual setting. Users must manually start new tasks.
Task start changed from Manual or Automatic to Discretionary	Might be supported.	If there are any existing regular task items with IBM Case Foundation process in waiting state, or in manual and ready state, the task process might not start, so the change is not recommended.
Task start changed from Discretionary to Manual or Automatic	No issues.	Existing tasks keep the existing Discretionary setting. New tasks use the new setting.
Changing the document type that is used in the **A document is filed in a case** precondition	No issues.	Affects new instances as well as existing instances that are in waiting state.
Changing the properties used in the **A case property is updated** precondition	No issues.	Affects new instances and existing instances that are in waiting state.
Required task setting	New cases are affected.	In the production environment, your IT administrator can run the case synchronizer utility for existing case instances to reflect new task settings as needed.
Repeatable task setting	No issues.	A task can be changed to repeatable as long as the precondition is either **A document is filed in a case** or **A case property is updated**.
Create new non-repeatable and non-discretionary (automatic or manually) task	New cases are affected.	Existing cases do not have the new task. In the production environment, your IT administrator can run the case synchronizer utility for existing case instances to reflect new task types as needed.

Table 18. Affects of solution design changes (continued)

Type of changes	Result	Comments
Add a new task within a container task	New and existing cases are affected.	If a container task has not started, it will include the new tasks. In the production environment, your IT administrator can run the case synchronizer utility for existing case instances to reflect new task types as needed.
Create new repeatable (File or Property update) task	New and existing cases are affected.	Existing cases will have the new task created when the document is filed or when property is updated.
Create new discretionary task	New and existing cases are affected.	Existing cases can also include the new task.
Add a new task to a group	New cases are affected.	Existing cases do not have the new task. In the production environment, your IT administrator can run the case synchronizer utility for existing case instances to reflect new task types as needed.
Remove a task from a group (change an inclusive or exclusive task to not grouped)	Only new cases are affected.	Existing cases with tasks that are required by an inclusive group or tasks that are disabled by exclusive group remain in the previous state and cannot be changed.
Move a task from one group to another (moving from no grouping to the inclusive group or exclusive group or changing the group)	Only new cases are affected.	Existing task instances maintain their grouping relationships.
Workflow name for a task	Not supported within Case Manager Builder.	Case Manager Builder uses the unique identifier for the task as the name of the workflow, and the unique identifier cannot be changed.
Launch step or page	Existing cases are affected.	The new page is used.
Workflow definition	Some existing cases are affected.	Any existing instances of tasks with workflows that have started are not affected. New tasks use the new workflow version.

Table 18. Affects of solution design changes (continued)

Type of changes	Result	Comments
Rule definition	Some existing cases are affected.	Any existing instances of tasks with workflows that have started and are past the step that invokes the rule are not affected. New or existing workflows that have not reached the step that invokes the rule use the new rule version.

Remember: Case Manager Builder uses the term *unique ID* for the Content Platform Engine symbolic name property. The unique ID is not the same as the Content Platform Engine ID property, which is a globally unique identifier (GUID).

Related tasks:

"Resetting the test environment" on page 26

Related reference:

"Synchronizing cases with solution data" on page 74

Synchronizing cases with solution data

If you modify a solution after it is deployed, run the case synchronizer utility to update existing instances to match the changes that you made.

By using the case synchronizer utility, you can update case instances to match changes that you make to the case type, such as:

- Adding new tasks
- Creating a new folder structure
- Updating the state of existing task instances in the case instances

The case synchronizer utility is in the IBM Case Manager installation folder.

Table 19. Case synchronizer file name and location

Platform	File name	Location
AIX	`caseSynchronizer.sh`	`/opt/IBM/CaseManagement`
Linux	`caseSynchronizer.sh`	`/opt/IBM/CaseManagement`
Linux for System z	`caseSynchronizer.sh`	`/opt/IBM/CaseManagement`
Windows	`caseSynchronizer.bat`	`C:\Program Files (x86)\IBM\CaseManagement`

Syntax

caseSynchronizer *command parameter-list*

parameter-list consists of a set of pairs, where each pair has a *parameter* and a *value*, separated by a space.

Commands

launch
Start the case synchronizer utility. The **launch** command requires parameters.

suspend
Stop the case synchronizer utility. The **suspend** command does not require parameters.

Parameters

-cews_uri
The web services URI to connect to Content Platform Engine, for example, http: //myserver:9080/wsi/FNCEWS40MTOM. This parameter is required.

-username
The user ID to connect to Content Platform Engine. This parameter is required.

-password
The password for the specified user ID to connect to Content Platform Engine. If the password is not specified, the case synchronizer utility will prompt for the password. This parameter is required.

-target_os
The target object store that the case synchronizer will check. This parameter is required

-caseType
The symbolic name of the case type for the tool to update. This parameter is required.

If the name of the case type includes spaces, surround the name with single quotation marks, for example, `-caseType 'Accident report'`.

-caseTypeFilter
The filter criteria to use when retrieving the case instances to update. This parameter is optional.

-includedTaskTypes
A comma-separated list of the task type symbolic names to add to the case instances. This parameter is optional.

-excludedTaskTypes
A comma-separated list of the task type symbolic names to exclude from the update to the case instances. This parameter is optional.

-file
The path to an input file that contains the parameters to run the tool. This parameter is optional.

If specified, the input file must include the **cews_uri**, **username**, **password**, **target_os**, and **caseType**parameters without leading hyphens.

-batchSize
The number of items to retrieve and process at one time. This parameter is optional. If not specified, the default batch size is 1000 items.

-threadPoolSize
The number of active threads for the tool to use when it processes case instances. This parameter is optional. The default value is 4.

For example, the following command starts the case synchronizer for cases of the type Accident Report and updates every case instance of that type with any changes that have been made to that case type.

```
caseSynchronizer launch -cews_uri http://myserver:9080/wsi/FNCEWS40MTOM
-username administrator -password mypassword
-target_os MyTargetOS -caseType 'Accident Report'
```

Verifying solution deployment

Verify your solution completely in your test and pre-production environments before you deploy the solution into production. After you deploy the solution, test the solution to verify that all of the components are working correctly.

Procedure

To verify the solution:

1. Log in to Case Manager Client.
2. From the list of available solutions, expand your solution, and click **Manage Roles**.
3. Click **Add Case** to add a case to the solution. Verify that the preconditions for the case are met.
4. Open and complete a work item from the in-basket to verify that the page works correctly.
5. Verify that case types, tasks, and roles are created and working. To verify that the other components in the solution work correctly, open and test other pages and cases. You can search for cases by going to the case pages and searching for a case by date.

Configuring logging in IBM Content Navigator for the IBM Case Manager administration client and Case Manager Client

To configure logging for IBM Case Manager web applications, you must enable debugging on the IBM Content Navigator server and restart the IBM Content Navigator server.

Procedure

To configure logging settings in IBM Content Navigator:

1. Log in to the IBM Content Navigator administration desktop.
2. Click the **Settings** tab and then click the **Logging** subtab.
3. Set the logging level for the applications to **Debug**.
4. Click **Save** and then click **Close**.
5. Log out of the IBM Content Navigator administration desktop.
6. Restart the application server instance where IBM Content Navigator is deployed.

Related information:

Enabling server logging for IBM Content Navigator

IBM Content Navigator log files

Configuring logging in WebSphere Application Server for Case Manager Builder and the API application

Case Manager Builder and the IBM Case Manager API application log information to the WebSphere Application Server main log and trace log. You can redirect the WebSphere Application Server log to record information for these components in the IBM Case Manager log location. You can also change the logging levels in WebSphere Application Server.

About this task

You can use the logging settings in the WebSphere Application Server administrative console to redirect the logs to the IBM Case Manager log location.

To access the settings in the administrative console, click **Troubleshooting** > **Logs and trace**, and select your server name.

Procedure

To configure logging options for Case Manager Builder and the IBM Case Manager API application:

- Redirect the log:
  1. Click **Diagnostic Trace** and click the **Runtime** tab.
  2. In the **File Name** field, change the value to *installation_path*/IBM/CaseManagement/logs.
- Redirect the main application server logs:
  1. Click **JVM logs** and click the **Runtime** tab.
  2. In the **File Name** fields, change the path before the /SystemOut.log and /SystemErr.log file names to the IBM Case Manager log location. For example, use *installation_path*/IBM/CaseManagement/logs/SystemOut.log and *installation_path*/IBM/CaseManagement/logs/SystemErr.log.
- Change the logging level:
  1. From the WebSphere Application Server administrative console, click **Logging and Tracing** > *server* > **Change log detail levels**.
  2. Change the logging levels as needed.

  Case Manager Builder components have the Message and Trace Levels set to info by default. Reset these components to audit or warning to prevent filling log files too quickly. Under the com.ibm.acm.* component, select the com.ibm.acm.sold.* node to set the **Message and Trace Levels** settings for all the Case Manager Builder components.

Configuring logging in WebLogic Server for Case Manager Builder and the API application

If you use Oracle WebLogic server, you can change the logging level and log location for Case Manager Builder and the IBM Case Manager API application by editing a file that is provided by IBM Case Manager.

About this task

To change the logging level and log location, edit a `log4j.properties` file that is provided in the *IBMCaseManager_home*`\configure\lib` directory. The following example `log4j.properties` file sets the location for log files to the `C:\Program Files\IBM\CaseManagement\logs\` directory.

For Case Manager Builder, the logging level is set to `INFO` and log entries are written to the `CaseBuilder.log` file. For the IBM Case Manager API application, the logging level is set to `INFO` and log entries are written to the `CaseAPI.log` file. You can set the logging level to `AUDIT` or `WARNcING` to prevent filling log files too quickly.

```
# log location
log = C://Program Files//IBM//CaseManagement//logs//

# log for Case Builder
log4j.category.com.ibm.acm = INFO,CaseBuilder
log4j.additivity.com.ibm.acm = false

# log for Case API
log4j.category.com.ibm.casemgmt = INFO,CaseAPI
log4j.additivity.com.ibm.casemgmt = false

# default
log4j.rootLogger = INFO,defaultAppender
log4j.appender.defaultAppender = org.apache.log4j.ConsoleAppender
log4j.appender.defaultAppender.layout = org.apache.log4j.PatternLayout
log4j.appender.defaultAppender.layout.ConversionPattern = %-4r [%t]
%-5p %c %x - %m %n

#Define appender for Case Builder
log4j.appender.CaseBuilder = org.apache.log4j.RollingFileAppender
log4j.appender.CaseBuilder.File = ${log}/CaseBuilder.log
log4j.appender.CaseBuilder.MaxFileSize = 2MB
log4j.appender.CaseBuilder.MaxBackupIndex = 2
log4j.appender.CaseBuilder.layout = org.apache.log4j.PatternLayout
log4j.appender.CaseBuilder.layout.ConversionPattern = %5p [%t] (%F:%L) - %m %n

#Define appender for CaseAPI
log4j.appender.CaseAPI = org.apache.log4j.RollingFileAppender
log4j.appender.CaseAPI.File = ${log}/CaseAPI.log
log4j.appender.CaseAPI.MaxFileSize = 2MB
log4j.appender.CaseAPI.MaxBackupIndex = 2
log4j.appender.CaseAPI.layout = org.apache.log4j.PatternLayout
log4j.appender.CaseAPI.layout.ConversionPattern = %5p [%t] (%F:%L) - %m %n
```

Procedure

To configure logging for Case Manager Builder and the IBM Case Manager API application:

1. Copy the log4j-1.2.15.jar file from the *IBMCaseManager_home*\configure\lib folder to the *Weblogic_home*\Middleware\user_projects\domains*IBMCaseManager_domain*\lib folder.
2. Extract the log4j.properties file and copy it to any location. Make a note of the path where you copied the file, such as c:\Cblog\log4j.properties.
3. Edit the log4j.properties file:
   a. Specify your preferred log file location (the path where you want the log files to be created).
   b. For Case Manager Builder, specify your preferred logging level (the amount of detail to be written to the log file) and a file name for the log file, such as CaseBuilder.
   c. For the IBM Case Manager API application, specify your preferred logging level and a file name for the log file, such as CaseAPI.
4. Edit the setDomainEnv.cmd file in the *Weblogic_home*\Middleware\user_projects\domains*IBMCaseManager_domain*\ folder.
5. Locate the following statement in the file:

```
if NOT "%LOG4J_CONFIG_FILE%"=="" (
set JAVA_PROPERTIES=%JAVA_PROPERTIES%
 -Dlog4j.configuration=file:%LOG4J_CONFIG_FILE%
```

6. Insert the following property before the preceding statement to set the path that you specified for the log4j.properties file in step 2. For example:

```
set LOG4J_CONFIG_FILE=c:\Cblog\log4j.properties
```

7. Save and close the file and then restart the application server The log files are generated by the name and location specified in the log4j.properties file, for example, C:\Program Files\IBM\CaseManagement\logs\CaseBuilder.log.

Modifying the size and location of Case Manager Builder CBE log files

You can modify the size and location of the Common Base Event (CBE) log files that are generated by Case Manager Builder. Because the log files are updated frequently, you might want to control how large they grow and change the default location. Information in this procedure applies to WebSphere Application Server, not Oracle WebLogic Server.

About this task

When you use Case Manager Builder to open, copy, close, or deploy a solution, the same information is written to two log files by default:

- icm/icm_casebuildercbe%g.log
- icm/icmcbe%g.log

The icm path is relative to the profile directory of your application server. For example, the path might be `/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/icm`.

%g Is the generation number to distinguish rotated logs. When the log file reaches a certain size, a new file is created with a file name that increments numerically, such as `icmcbe0.log`, `icmcbe1.log`, and so on.

icmcbe%g.log
Is a log file that is created by the IBM Case Manager API. Because Case Manager Client uses the IBM Case Manager API, any activity in Case Manager Client generates events that are logged in this file.

icm_casebuildercbe%g.log
Is a log file that is created by Case Manager Builder. Because Case Manager Builder uses the IBM Case Manager API, this log file might contain entries that are also in the `icmcbe%g.log` file.

You can change the log level for the IBM Case Manager API and Case Manager Builder CBE log files to reduce the size the files or to capture more or less information than what the default logging level provides. If you do not want to generate any CBE log files, you can also turn off logging entirely.

IBM Case Manager configuration tool sets the -DICMCBELogFilePattern=icm/icmcbe%g.log property during the Deploy Case Manager API task. This setting redirects the content-logged entries that otherwise would go into `icm_casebuildercbe%g.log` file to the `icmcbe%g.log` file resulting in one log file instead of two log files. You can modify this property to change the location of the log file.

Procedure

To modify log file options for the CBE log files:

- Modify the log file location and generate one log file instead of two log files:

1. In the WebSphere Application Server administration console, add the ICMCBELogFilePattern property to the Java Virtual Machine (JVM) configuration settings. Click **Application servers** > *server* > **Process definition** > **Java Virtual Machine**.
2. In the **Generic JVM arguments** field, modify the ICMCBELogFilePattern property to create a single log file. In the following example, a single log file (`icmcbe%g.log`) is created in the system temporary directory (`%t`, for the `/tmp` directory on AIX, Linux, or Linux on system Z):

   ```
   -DICMCBELogFilePattern=%t/icmcbe%g.log
   ```

   If you prefer, you can direct the logging to a specific folder, such as `/icm/logs`. For example, specify `-DICMCBELogFilePattern=/icm/logs/icmcbe%g.log` (for AIX, Linux, or Linux on system Z) or `-DICMCBELogFilePattern=C:\icm\logs\icmcbe%g.log` (for Windows).

   Restriction: WebSphere Application Server does not create folders for you. The folder that you specify for the log files must already exist. For example, if you direct the log files to the `C:\icm\logs\` folder, you must ensure that the `icm\logs` folder exists on the C: drive.
3. Save your changes and restart WebSphere Application Server. When you use Case Manager Builder to copy a solution, for example, the log files are written in the location that you specified. Using `icmcbe%g` as the sample file name, the first log file is named `icmcbe0.log`, followed by the `icmcbe1.log`, and so on.

- Modify the maximum size of the log files:
  1. In the WebSphere Application Server administration console, add the ICMCBELogMaxSize property to the Java Virtual Machine (JVM) configuration settings. Click **Application servers** > **server** > **Process definition** > **Java Virtual Machine**.
  2. In the **Generic JVM arguments** field, modify the ICMCBELogMaxSize property to control the maximum size of the log, in bytes. By default, the maximum log file size is 500 MB (524288000 bytes). In the following example, the maximum log file size is 500 MB:

     ```
     -DICMCBELogMaxSize=524288000
     ```
  3. Save your changes and restart WebSphere Application Server. When the log file reaches a size of 5 MB, it is renamed from `icmcbe0.log` to `icmcbe1.log`, and a new log file is started with the name `icmcbe0.log`.
- Modify the maximum number of log files:
  1. In the WebSphere Application Server administration console, add the ICMCBELogCount property to the Java Virtual Machine (JVM) configuration settings. Click **Application servers** > **server** > **Process definition** > **Java Virtual Machine**.
  2. In the **Generic JVM arguments** field, modify the ICMCBELogCount property to control the maximum number of logs. By default, the maximum number of logs is 5. In the following example, the maximum number of logs is 5:

     ```
     -DICMCBELogCount=5
     ```
  3. Save your changes and restart WebSphere Application Server. When five log files are written and the newest log file reaches the maximum log file size, the oldest log file is deleted.
- Change the logging level for IBM Case Manager API and Case Manager Builder CBE files:
  1. From the WebSphere Application Server administrative console, click **Logging and Tracing** > *server* > **Change log detail levels**.

2. Under the com.ibm.casemgmt.* component, select the com.ibm.casemgmt.cbe node and set the message and trace levels as needed. The default logging level is `info`. Select No Logging to disable logging, or change the settings to `audit` or `warning` to prevent filling log files too quickly.
3. Save your changes and restart WebSphere Application Server.

Troubleshooting IBM Case Manager administration

Troubleshoot typical errors that might surface in IBM Case Manager administration.

Related troubleshooting information

"Database deadlock issue with large solution deployments" on page 201
"Event payloads can contain model objects that are not fully retrieved" on page 202
"EAR file for custom widget package isn't deployed" on page 204
"IBM Case Manager configuration tool task fails with 414 error" on page 205
"Re-creating an IBM Case Manager target object store in a development environment" on page 206
"Configure Box Collaboration task fails in a distributed environment when the date/time is not synchronized" on page 209

Related concepts

"Improve performance at case creation time by limiting subfolder structure" on page 202
"IBM Case Manager administration client does not remove all files that are related to the package" on page 203
"Older versions of an audit or security configuration in the IBM Case Manager administration client might not be re-imported" on page 204

Related tasks

"Removing proxy documents that are associated with external documents" on page 192
"Supporting external documents in production environments" on page 203

Fixing unreadable characters in AIX for a locale other than English in the IBM Case Manager configuration tool

You might see unreadable characters in the IBM Case Manager configuration tool when it is started with a locale other than English.

Symptoms

If you start the IBM Case Manager configuration tool in AIX with a locale other than English, the IBM Case Manager configuration tool might display unreadable characters.

Resolving the problem

Before you start the IBM Case Manager configuration tool, set the locale to whatever locale you want to use by entering the following commands on the IBM Case Manager server:

```
export LC_ALL=locale
export LANG=locale
```

locale is the locale that you want to use.

You can get a list of the available locales on your system by running the following command: `locale -a`.

To avoid getting unreadable characters, use a locale that uses the UTF-8 encoding. For example, for the French locale, enter the following command:

```
export LC_ALL=FR_FR.UTF-8
export LANG=FR_FR.UTF-8
```

For a list of the common locales that can be used with IBM Case Manager configuration tool in AIX, see Supported languages and locales.

Display issues with IBM Case Manager configuration tool

You might encounter display issues with drop-down lists if you are using IBM Case Manager configuration tool on Red Hat Enterprise Linux with OpenText Exceed (formerly, Hummingbird Exceed).

Symptoms

The items in the drop-down list do not display correctly. For example, the drop-down list does not display any entries.

Resolving the problem

To resolve the problem:

1. Close the IBM Case Manager configuration tool and restart.
2. If you continue to have display problems, use different X server client software to connect to the configuration tool, such as X-Ming or Cygwin-X.

IBM Case Manager configuration tool returns an SSLHandshakeException error

The IBM Case Manager configuration tool can connect to a server by using a Security Socket Layer (SSL) or Transport Layer Security (TLS) connection. However, the configuration tool returns an SSLHandshakeException error if the SSL signer or TSL signer is not added to the keystore.

Symptoms

When the IBM Case Manager configuration tool connects to a server by using an SSL or a TLS connection, the certificate of that server is verified against the keystore that is used by the configuration tool. To ensure that the server certificate is authentic and that a malicious entity is not trying to impersonate the server, you must add self-signed certificates to the JVM for the IBM Case Manager configuration tool. These certificates are required for https connections.

If you do not add an SSL signer or a TSL signer to the keystore, IBM Case Manager configuration tool returns an error when a connection attempt is made. This error takes the following form:

```
javax.net.ssl.SSLHandshakeException: com.ibm.jsse2.util.j:
      PKIX path building failed:
    java.security.cert.CertPathBuilderException:
```

Because http connections are not encrypted, you do not need to add keys for certification authority (CA) certificates that use an http connection.

Resolving the problem

You might need to add certificates for the Content Platform Engine load balancer or server and the IBM Content Navigator load balancer or server. Before you begin, ensure that Content Platform Engine and IBM Content Navigator are already configured for SSL or TSL.

To add an SSL signer or a TSL signer to the keystore for the IBM Case Manager configuration tool:

1. For each certificate that you need to add to the keystore, obtain the certificate from the server to which the configuration tool is connecting.
   a. On the Content Platform Engine server, log in to the WebSphere Integrated Solutions Console.

b. Click **Security** > **SSL certificates and key management**.

c. Open the Signer Certificates page:

Option	Description
WebSphere Application Server cluster configuration	Click **Key stores and certificates** > **CellDefaultTrustStore** > **Signer certificates**.
WebSphere stand-alone configuration	Click **Key stores and certificates** > **NodeDefaultTrustStore** > **Signer certificates**.

d. Under **Additional Properties**, select **Signer certificates**.

e. Select the check box next to the certificate to export and click **Extract**.

f. Enter a name and the location where the extracted certificate file is to be stored, and then click **OK**.

2. Add each certificate to the keystore for the IBM Case Manager configuration tool.

a. Start IBM Key Management by entering one of the following commands from the command line:

Option	Description
AIX®, HPUX, HPUXi, Linux, Linux on System z®, Solaris	`_install_path/java/sdk/jre/bin/ikeyman.sh`
Windows	`_install_path\java\sdk\jre\bin\ikeyman.bat`

b. Click **Keybase File** > **Open**.

c. For the **Key database type**, select **JKS**.

d. Click **Browse** and navigate to `_install_path/java/sdk/jre/lib/security/cacerts`.

e. Click **OK**.

f. Enter the password and click **OK**. The default password is `changeit`.

g. Add the certificates that you exported in step 1 to the trust file for IBM Case Manager configuration tool.

h. Close IBM Key Management.

Solution export problems

Various problems can occur when exporting a solution from IBM Case Manager.

Symptoms

When you export the solution, the IBM Case Manager administration client displays a message like one of the following messages:

```
The solution could not be exported because of the following error: EXPORT failed.
0 items processed: 0 succeeded, 0 failed. Apache Derby experienced a sql exception.
Create table tablename. A lock could not be obtained within
 the time requested. FNRAM9042
```

```
The solution could not be exported because of the following error: EXPORT failed.
0 items processed: 0 succeeded, 0 failed. Apache Derby experienced a sql exception.
Create table tablename(hashcode int, mapkey varchar(76),
mapdata varchar(32672)) Table/View 'TABLENAME' already exists
in Schema 'APP'.  FNRAM9042
```

```
The solution could not be exported because of the following error: EXPORT failed.
42 items processed: 42 succeeded, 0 failed. An unexpected exception occurred. The
unexpected exception is chained to this exception. A lock could not be obtained
within the time requested  FNRAM9042
```

Causes

These export problems can be caused by two or more users exporting a solution at the same time.

- When you export a solution, you might encounter Derby or SQL errors if another user tries to export a solution on the same system at the same time.
- (For WebSphere Application Server on AIX or Linux only) You might be unable to export a solution if two users previously attempted to export two solutions at the same time.

Resolving the problem

To resolve the problem:

- If you are exporting a solution while someone else is also exporting a solution, wait until the other solution is exported and try the operation again.
- If you can't export a solution because of a previous simultaneous export attempt, delete the WebSphere Application Server folder `/opt/IBM/WebSphere/AppServer/derby/P8DerbyTmpDB`. Then, try the export again.

Solution import problems

Various problems can occur when importing a solution to IBM Case Manager or when deploying a solution.

Symptoms

You might experience the following symptoms:

1. When you import the solution, the IBM Case Manager configuration tool displays the following message:

   ```
   A uniqueness requirement has been violated.
   The value for property ContainmentName of class
   DynamicReferentialContainmentRelationship is not unique.
   ```

2. Case Manager Builder displays the imported solution as being out of sync or as already deployed even though you did not yet deploy the newly imported solution.
3. When you deploy the imported solution, you receive the following error message:

   ```
   FNRPA0037E The page that is associated with the step
    processor cannot be found because no page ID exists for the
    page name page.
   ```

   You receive this error for every page that is missing from the solution package.

Causes

This import problem can be caused by one or more of the following:

1. The solution that you are importing has the same name as an existing solution and the objects in the solutions have the same name but different GUIDs. For example, if you import a solution into the production environment and then delete pages from the solution with the same name in the development environment and export the pages again, importing the solution fails because now the pages have the same name but different GUIDs.

2. A newly imported solution displays as deployed because a previous version of the solution might have been deployed, and Case Manager Builder is displaying the status of the previously deployed solution for the newly imported solution.
3. The solution package is missing one or more pages.

Diagnosing the problem

To diagnose the problem:

1. See the IBM Case Manager configuration tool debug trace logs and the FileNet P8 error logs, which will list the GUIDs of the problem objects in the full stack trace. The IBM Case Manager configuration tool log file is located in the `/logs` directory in the location where you installed IBM Case Manager. If you use WebSphere Application Server, the FileNet P8 server log files are located in `<WAS_install_location>/WebSphere/AppServer/profiles/<AppServer01>/FileNet/server1`. If you use Oracle WebLogic Server, consult the WebLogic documentation or your system administrator for the location of the log file.
2. If you removed a solution from the design object store and then reimported that solution into the same environment or you copied a solution that you previously removed back into the same environment, Case Manager Builder might display the newly imported solution as deployed even though it is not deployed. Case Manager Builder might also show the copied solution to be out of sync.
3. Compare the pages of the imported solution with the source solution on the original development environment to determine what pages need to be regenerated.

Resolving the problem

To resolve the problem:

1. If you are importing a solution that already exists in the system, ensure that the common objects between the solution that you are importing and the solution in the system have matching GUIDs.
2. Reinitialize the target object store to remove the previously deployed solution and deploy your solution again.
3. If the solution package is missing pages, compare the pages of the imported solution to the source solution on the original development environment then redeploy the solution to the original development environment to ensure that the solution successfully deploys. Also, ensure that all of the pages are generated. Export the solution package again and import and deploy the solution to the target environment again.

Removing invalid principal mappings after a solution is imported

After you import a solution, you receive a message that the imported solution includes principal mappings that cannot be displayed.

Symptoms

After you import a solution package by using the IBM Case Manager administration client, you receive an informational message such as the following message:

```
2 principal mappings that cannot be displayed are included in the solution import.
```

Causes

The imported solution contains references to an LDAP user that was deleted from the LDAP server.

Resolving the problem

Review the principal mappings for the imported solution and remove any principal mapping for which the display name is set to **Invalid Principal**. In the Administration Console for Content Platform Engine, select your design object store and select the folder for your solution. On the **Security** tab, remove any entry whose name is **Invalid Principal**.

Tip: If security permissions are set on individual assets in your solution, select each asset in the folder and review its security permissions.

Unable to access the role assignment page from the Deploy Solution task

The **Assign Roles** button on the Deploy Solution task accesses the Case Manager Client URL. If your browser type is not compatible, the configuration tool cannot start the embedded browser.

Symptoms

When you click the **Assign Roles** button, the IBM Case Manager configuration tool fails to access the Case Manager Client URL in an embedded browser.

Resolving the problem

Verify that you have the supported Mozilla version for Eclipse V3.7.2, which is the version of Eclipse that is used by the IBM Case Manager configuration tool. You might also need to configure your MOZILLA_FIVE_HOME environment variable and your LD_LIBRARY_PATH environment variables. For details, see one of the following links:

- What do I need to run the SWT Browser inside Eclipse on Linux?
- What do I need to run the SWT Browser in a standalone application on Linux or Solaris?

Solution export fails with an Apache Derby SQL exception

If you receive an Apache Derby SQL exception error when exporting a solution, you must remove the Apache Derby database folder.

Symptoms

You receive the following error when exporting a solution:

```
Apache Derby experienced a sql exception.
```

Causes

A previous solution export failed, which left the Apache Derby database that is used by the IBM Case Manager administration client to export that solution. The database is not removed when a solution export fails because the database is retained for diagnostic purposes. When another solution is exported, the database that was left from an earlier solution export is reused, which causes the Apache Derby SQL exception.

Resolving the problem

Remove or rename the `P8DerbTmpDB` folder in *`install_path`*`/configure/tmp_sp/P8DerbyTmpDB.` directory, and then try exporting the solution again.

Deleting a case

Use the IBM Administration Console for Content Platform Engine to delete a case.

Symptoms

You delete the case folder but the case is not completely removed. Some case items remain in the system.

Resolving the problem

Deleting a case comprises the following two main tasks:

1. Promoting the case tasks and deleting the work items.
2. Deleting the case folder.

Important: When you delete a case, all of the open work items, tasks, and comments that are associated with the case are removed.

Restriction: Deleting a case is not supported in a production environment because doing so can cause reference problems and compromise security.

To promote the case tasks and delete the case work items, complete the following steps:

1. In IBM Administration Console for Content Platform Engine, navigate to the appropriate domain, expand **Object Stores**, and click the name of the IBM Case Manager target object store that contains the case that you want to delete.
2. After expanding the folders in the target object store, navigate to **Browse** > **Root folder** > **IBM Case Manager** > **Solution Deployments** > **My Solution** > **Case Types** > **Cases**.
3. Navigate to the task sequence folder: **Year** > **Month** > **Day** > ***number*** > ***task_sequence***.

   For performance reasons, cases created on the same day are filed under a folder with a random number between 0001 and 0300. For example, **2013** > **07** > **19** > **0166** > **000000100003**. If a large number of cases are filed on the same day, you might need to use the Search function of the Administration Console for Content Platform Engine and search the target object store to find the case.
4. Left-click the ***task_sequence***. In the pane on the right, click the **Tasks** tab.
5. In the **State** column, complete the following actions for tasks that are in **Failed** or **Working** state:
   a. Click the task.
   b. Click the **Properties** tab.
   c. If the task is in the **Failed** state, and the value of the **Disabled State** property is **3**, ignore this step and continue with step 6.
   d. For **Failed** or **Working** tasks that are not disabled, scroll down to the **ID** field and record its value. You will need the task ID in a later step when you remove the corresponding workflow.
   e. Go back to the ***task_sequence*** tab and close the task tab.
   f. Click **Promote State**. Verify that the task state is **Complete**.
6. On the **Tasks** tab, select each task that is in **Waiting** or **Ready** state, and then click **Delete**.
7. Close the window.
8. Open the Process Administrator by going to ***IBM Case Manager_target object store*** > **Administrative** > **Workflow System** > **Connection Points** >

connection_point. Right-click the connection point and select **Administer Work Items**. The administration *connection_point* window is displayed.

9. In the **Look for** field, select **Workflows**.
10. In the **In** field, select **Workflow Roster**, which is the same name as the solution.
11. In the **Search mode** field, select **Edit (all fields)**.
12. Click **Find Now**.
13. Click **View** > **Show/Hide Columns**.
14. In the **Column Selection** window, add **F_CaseTask** to the **Selected Columns** field, and then click **OK**. Verify that **F_CaseTask** is displayed in the **Results** window.
15. Use the task ID from step 5d on page 188 to identify the workflow that is associated with each of the tasks that you promoted earlier. Right-click the workflow and then click **Tasks** > **Delete Work**.
16. Click **OK** to confirm that you want to delete the work item or items.

To reuse documents from deleted cases, you must remove the reference to the Associated Case object in the document property before you delete the case. Otherwise, you will be unable to update properties on the supporting documents from deleted cases.

1. In Administration Console for Content Platform Engine, navigate to the task sequence folder: **Year** > **Month** > **Day** > ***number*** > ***task_sequence***. For example, **2013** > **07** > **19** > **0166** > **000000100003**.
2. Left-click the ***task_sequence***. In the pane on the right, click the **Contents** tab and navigate to the supporting document folder, such as Correspondence.
3. Left-click the document. In the new middle tab, select the **Properties** tab.
4. Scroll down, left-click the arrow next to the **Associated Case** property value, and select **Unset Value**. Click **Save**.
5. In Administration Console for Content Platform Engine, right-click the **task_sequence** (such as 000000100003), and then click **Delete**.
6. Click **OK**.

To remove the case folder, complete the following steps:

1. In Administration Console for Content Platform Engine, navigate to the task sequence folder: **Year** > **Month** > **Day** > ***number*** > ***task_sequence***. For example, **2013** > **07** > **19** > **0166** > **000000100003**.
2. Right-click ***task_sequence*** and then click **Delete**.
3. Select **Delete all objects and their content elements from all folders** and then click **OK**.

Removing a case type

When you remove a case type, you must also remove the case type folder structure.

Symptoms

You removed a case type from a solution and then redeployed the solution. The case type that you removed still displays in Case Manager Client.

Causes

When you deploy a solution, IBM Case Manager creates a solution folder structure that contains the case type names for all of the case types in the solution. When

you redeploy the solution, the case type that you removed does not get removed from the folder structure. Case Manager Client displays the case types for the solution that use the entries in the folder structure.

Resolving the problem

Complete the following steps to remove the case type:

1. In Case Manager Builder, open the solution that contains the case type that you want to remove.
2. Remove the case type and then save the solution.
3. Deploy the solution.
4. In IBM Administration Console for Content Platform Engine, delete the folder structure for the case type that you want to remove.
   a. Expand **Object Stores** and click the target object store in which the solution resides.
   b. In the navigation pane for the target object store, expand **Browse** > **Root Folder** > **IBM Case Manager** > **Solution Deployment** > *solution* > **Case Types**.
   c. Right-click the case type that you want to remove and click **Delete**.

When a solution name exceeds 58 characters, the work items in the solution do not display in a personal in-basket after the solution is deployed

When you enter the solution name in the IBM Case Manager configuration tool or in Case Manager Builder, ensure that the name is 58 characters or fewer. Otherwise, the work items will not display in a personal in-basket after the solution is deployed.

Symptoms

If your solution name exceeds 58 characters, the work items do not display in a personal in-basket after the solution is deployed.

Causes

When you use the IBM Case Manager configuration tool to create a solution from a solution template or copy a solution from another solution , you can enter as many characters as you want for the solution name. When you use Case Manager Builder to create a solution, you can enter up to 64 characters for the solution name.

Resolving the problem

Change the length of the solution name by modifying the SolutionIdentifier value in Process Designer. If you did not yet deploy the solution, complete the following steps to change the length of the SolutionIdentifier:

1. In Process Designer open the solution.
2. Click **View** > **Configuration**.
3. Right-click the **Inbox** queue and select **Properties**.
4. Open the **Data Fields** tab.
5. Change the length of the **SolutionIdentifier** data field to a new value.

   The new value is calculated by adding the length of the solution name and six additional characters.
6. Save the solution.

If the solution is deployed, complete the following steps to change the length of the SolutionIdentifier property in the Process Configuration Console:

1. In Process Configuration Console, connect to the Process Engine isolated region.
2. Right-click the Inbox queue and select **Properties** .
3. Open the **Data Fields** tab.
4. Change the length of the **SolutionIdentifier** data field to a new value.

   The new value is calculated by adding the length of the solution name and six additional characters.
5. In Process Configuration Console, commit the change.

Solution deployment fails with a Process Engine views error

Your solution deployment fails if the length of your solution name, role name, case type name, or field name exceeds the limit of the database view name that is set by the Process Engine database. This issue is specific to Oracle databases.

Symptoms

You receive the following error message: `ERROR FNRPA0032E The solution cannot be deployed because the Process Engine configuration document could not be imported. See the following error: Cannot create new views; old views deleted. Run transfer or re-create views. The old database views for queues, rosters, and event logs have been deleted, but the new views could not be successfully created. The transfer or view creation option must be done again to properly create the views, after whatever problem that caused view creation to fail has been fixed. See the chained exception for the problem that caused the view creation to fail. java.lang.Exception: ORA-00972: identifier is too long`

Causes

One or all of the following solution elements is too long: solution name, role name, case type name, or field name. Process Engine generates the database view names for the event log that maps to the case type unique name, the queue that maps to the role unique name, the roster that maps to the solution name, and field name. If the view name is too long, Process Engine automatically truncates the view name to be within 30 characters.

However, even with automatic truncation, the database view names might still exceed 30 bytes, the restriction set by the Oracle database, if a character is more than 1 byte.

Resolving the problem

Use Case Manager Builder to assign a shorter name for the solution, role, case type, or field name. The name limits are documented in the FileNet P8 product documentation. After you shorten the names and save the solution, redeploy the solution.

Related information

Naming conventions

Cannot see changes to assets such as document types or properties in Case Manager Client

Case Manager Client users cannot see changes to assets that were recently added or modified by using Case Manager Builder.

Symptoms

In Case Manager Builder, you updated your case by adding or modifying assets such as document types, case types, case type properties, property constraints, or choice list items. Your changes are visible in Case Manager Builder. You redeployed your solution and then try to use the new or modified asset in Case Manager Client, but you do not see the additions or modifications.

Causes

A newly added or modified asset does not immediately display in Case Manager Client because there is a delay when displaying new or modified assets such as document types or property constraints. The delay time is determined by the **CPE Metadata Cache Time to Live** setting in the Register the IBM Case Manager Services Plug-in task in the IBM Case Manager configuration tool. If no value is specified for the **CPE Metadata Cache Time to Live** setting, the default values of 5 seconds in the development environment and 36000 seconds (10 hours) in the production environment are used.

Resolving the problem

In the configuration tool, run the Register the IBM Case Manager Services Plug-in task and set a lower value for the **CPE Metadata Cache Time to Live** setting. Then, restart IBM Content Navigator.

In a production environment, restart the Content Platform Engine and IBM Case Manager servers after a solution is deployed or redeployed.

Removing proxy documents that are associated with external documents

When you unfile an external document from a case, the associated proxy document is not removed from the case management object store. To remove the proxy document, manually delete it from Content Platform Engine by using IBM Administration Console for Content Platform Engine.

About this task

To remove one or more proxy documents:

Procedure

1. Use IBM Administration Console for Content Platform Engine to open the target object store.
2. Select the **Search** node, then open a new search.
3. In the **Simple View** tab, select **External Document class**.
4. In the **SQL View** tab, add the following `WHERE` condition before the `OPTIONS` condition: `WHERE [CmAcmAssociatedCase]IS NULL`
5. Run the search.
6. In the **Search Results** tab, select all unreferenced proxy documents and then select the **Batch Operations** action.

7. Select the **Delete** option, click **OK**, and then confirm the deletion.

Cannot reassign work items in the All Assigned Work in-basket

To reassign work items in the All Assigned Work in-basket, your role must have the appropriate permissions.

Symptoms

You can see all work items in the All Assigned Work in-basket, but you cannot reassign the work items.

Causes

Your role does not have the permission to reassign work.

Resolving the problem

Ask your administrator to take one of the following actions:

- In Case Manager Client, go to **Manage Roles**, and add you to a role that has permission to reassign work.
- In Case Manager Builder, go to the **Roles** tab, and locate your role. For the **Work assignment options to display for this role** section, select the **Role members can reassign work to others** option.

Messages and annotations in the viewer are not displayed according to the browser locale setting or are not displayed correctly

When you view documents by using Case Manager Client, the messages and annotations in the viewer are not displayed in the locale in which the browser is set, or they are displayed incorrectly.

Symptoms

Messages and annotations are not displayed in the locale in which the browser is set, or they are displayed incorrectly.

Causes

The viewer that is used to display the messages and annotations uses the regional settings of the client system to determine the locale in which to display the messages and annotations instead of using the browser locale, which is the expected behavior.

This occurs in the default viewer when you view documents that are stored in Content Platform Engine, and the IBM Content Navigator viewer when you view documents that are stored in Content Platform Engine or IBM Content Manager. This issue does not apply to the default viewer when you view documents that are stored in IBM Content Manager because it does not support annotations and messages.

Resolving the problem

1. Go to **Control Panel** > **Regional and Language Options** and in the Standards and formats section, select a language, and then click **OK**. The window closes.
2. Go to **Control Panel** > **Java** and clear the cache.
3. Clear your browser cache.
4. Reopen your document.

Unlocking a locked work item

A work item can get locked if a user does not complete the work item and does not go back to complete the item, or if a user closes the browser before completing the work item.

Symptoms

A work item is locked by another user and you cannot modify it or reassign it. A lock icon is displayed next to a locked work item and the reassign option is disabled for the work item.

Causes

A work item owned by user A can be locked if:

- User A does not complete a work item because user A might be on vacation or left the company.
- User A closes the browser before he or she completes the work item.

Diagnosing the problem

A lock icon displays next to a locked work item and the reassign option is disabled for the work item.

Resolving the problem

To unlock a locked work item:

1. In FileNet Process Administrator, search for the work item, and then select the work item to unlock it.

After you unlock the work item, you can reassign the work item to another user by using Case Manager Client.

Business analysts should not select and bring reused long string properties into the search view of a case type

A search in Case Manager Client that uses long string properties might have invalid operators that are causing the Case Manager Client search to fail.

Symptoms

If long string properties are exposed, some operators are not valid, and the search will fail. Only `Starts with`, `ends with`, `contains`, `is empty`, and `is not empty` are the valid operators.

Causes

When designing your solution, you selected to reuse a long string property from Content Platform Engine, and then exposed that long string property in the search view of a case type, which uses an equal operator during search execution. However, the `begins with`, `ends with`, `contains`, `is empty`, and `is not empty` operators are the only valid operators for a long string property and cause the failure in a Case Manager Client search.

Resolving the problem

Business analysts should not select and bring reused long string properties into the search view of a case type within Case Manager Builder to prevent an invalid search operation. When designing your solution, do not add a long string property into the **Case Search** view.

Adding workflow groups to a step in Process Designer can cause validation errors in Step Designer

You see validation errors in Step Designer for a workflow that validated successfully in Process Designer.

Symptoms

When you start Process Designer from the Tasks page, add a workflow group, and assign the group to a step, the workflow validates in Process Designer. When you return to Step Designer, the workflow causes validation errors.

Causes

When you add a workflow group in Process Designer, and assign the group to a new step, the workflow can be validated in Process Designer. However, the workflow group is not added to the XPDL file immediately. When you try to validate the same workflow in Step Designer, you see a validation error for exposing the workflow group and for adding the group to the step.

Resolving the problem

To validate the new workflow in Step Designer, save and close the solution in Case Manager Builder. Reopen the solution and validate the workflow in Step Designer. The workflow validates successfully.

Related concepts

"Cannot access Process Designer from Case Manager Builder with Google Chrome" on page 230

Changing the saved solution locale after solution deployment

If you deploy a solution under the wrong locale the first time that you deploy it, the wrong solution locale is saved to the target object store for that solution. To resolve the problem, you must manually change the solution properties in the target object store.

Symptoms

The display names, such as case properties, case types, tasks, and other solution artifacts are not preserved and are not displayed correctly in the Case Manager Client. You can lose your translated display names.

Causes

The solution was deployed to a target environment under a locale that does not match the solution locale.

When you design and create a solution, you must decide what the solution locale is. The solution locale refers to the locale of display names, such as case properties, case types, tasks, and other solution artifacts that you create with Case Manager Builder. When you deploy the solution to a target environment for the first time, you must deploy the solution under the same locale to ensure that the display names are preserved.

The locale that is used the first time that you deploy a solution persists in the target object store for that solution. Future redeployments always use the saved solution locale regardless the locale that you use for redeployment.

Resolving the problem

To prevent this problem, ensure that you deploy the solution under the designated solution locale.

If you accidentally deploy the solution under a different locale, do the following steps to change the saved solution locale:

1. In the IBM Administration Console for Content Platform Engine, browse to **Target Object Store** > **Solution Deployments**, right-click your solution, and select **Properties**.
2. On the Properties tab, view the **Configuration** properties. Change the value of the **deploymentLocale** property to your locale code. For example, for German, change the default value, deploymentLocale=en_US, to deploymentLocale=de.
3. Deploy the solution again.

Problems occur when you import solutions with IBM FileNet Deployment Manager

Various problems can occur when you use FileNet Deployment Manager to import solution assets into IBM Case Manager.

Symptoms

You might experience the following symptoms:

1. You receive an error that states that the security principal was not found when the solution is imported by using the IBM Case Manager administration client.
2. LoggingStream errors are returned when the solution is imported:

```
2013-06-25 23:59:43,731 WARN [pool-5-thread-
1]filenet_error.api.com.filenet.apiimpl.imex.LoggingStream - The current
import process is attempting to update system properties and the current
user does not have security right to do this for object store
TOS01_cmicmint2vm15. Some or all of this import may fail until the
current user is assigned the "modify certain system properties" right on
the object store.

2013-06-25 23:59:44,121 ERROR [pool-5-thread-
1]filenet_error.api.com.filenet.apiimpl.imex.LoggingStream - Object has
failed the import process because of an error
classId=PropertyTemplateInteger32&objectId={AAD2FAB6-2708-4D0A-B590-
0156A03D130D}&objectStore={51D125E0-D03C-4808-9A41-4CEE42DCF245} Method
failed because an object or property is read-only. LastModifier is a
read-only property and cannot be updated at this time.
```

Resolving the problem

To resolve the problem:

- If you receive an error that the security principal was not found when you use the IBM Case Manager administration client to import the solution, use the IBM Case Manager configuration tool to import the solution. The IBM Case Manager configuration tool does not map security principals that are associated with solution assets.

  Alternatively, if you want to use the IBM Case Manager administration client to import the solution, disable principal mapping for imported assets:

  1. In the web client, open the IBM Content Navigator administration tool.
  2. Click **Plug-ins** > **IBM Case Manager administration plug-in**.
  3. Under **Additional Properties**, clear the **Allow target principal mapping when assets are imported** check box.

4. Save your changes.

- If the import operation fails due to LoggingStream errors, clear the **Use original create/update timestamps and users** check box on the FileNet Deployment Manager Import Options page.

  Alternatively, if you need to select the **Use original create/update timestamps and users** check box because you want to use the original time stamps from the source environment instead of new time stamps, grant the **Modify certain system properties** permission:

  1. In Administration Console for Content Platform Engine, open the IBM Case Manager design object store and select the **Security** tab.
  2. Select the user that does the import operation and click **Edit**.
  3. In the Edit Permissions window, select the **Modify certain system properties** check box.
  4. Save your changes.

Troubleshooting Kerberos SPNEGO single sign-on configuration

When creating the initial IBM Case Manager Version 5.2 deployment profile, you may receive an error message when you are setting the WebSphere Application Server properties for IBM Content Navigator.

Symptoms

The error message states that the Kerberos `krb5.ini` file cannot be found.

Causes

The IBM Case Manager configuration tool picks up the Kerberos configuration file from the Microsoft Windows system path by default.

Resolving the problem

Ensure that the Kerberos configuration file is copied to the default Windows system path. The default Kerberos configuration file on Windows is `/Windows/krb5.ini`. In a distributed environment, the file is located in `/etc/krb5.ini`. On a Windows Server 2008 system, the Kerberos configuration file is copied to the `C:\Windows` directory.

Alternatively, if you specify another location path for the Kerberos configuration file, then you must specify the `java.security.krb5.conf` JVM property in the IBM Case Manager configuration tool `configmgr.ini` file. For example, if your Kerberos configuration file (`krb5.ini`) is located in the `C:\SSO\`, then add the following line to the `configmgr.ini` file:

```
-Djava.security.krb5.conf=C:/SSO/krb5.ini
```

Related tasks

"Configuring IBM Case Manager to support SSO through Kerberos SPNEGO" on page 108

Troubleshooting CA eTrust SiteMinder single sign-on configuration

The **Register Project Area** task in the IBM Case Manager configuration tool fails and displays an error message stating that an error occurred while running Register Target Environment.

Symptoms

While completing configuration of IBM Case Manager with CA eTrust SiteMinder single sign-on, you receive an error message that states the following:

```
Starting to run Register Target Environment

Register Target Environment
Finished running Register Target Environment
An error occurred while running Register Target Environment
The task failed because of the following error:
Server returned HTTP response code: 500 for URL:
```

Causes

The maximum URL length allowed by the SiteMinder Web Agent is not long enough. The URL size that the IBM Case Manager configuration tool is trying to pass into the SiteMinder Policy Server via the SiteMinder Web Agent is larger than the default SiteMinder agent configuration **MaxUrlSize** of 4097 bytes.

Resolving the problem

In the SiteMinder Policy Server, try increasing the **MaxURLSize** parameter to 5120 in the SiteMinder Web Agent. If the error continues to occur, try increasing the **MaxURLSize** parameter to 8192 or higher.

Related tasks

"Configuring IBM Case Manager to support SSO through CA eTrust SiteMinder" on page 106

Cannot copy solutions that contain rule steps in a production environment

In a production environment, when you try to copy a solution that contains a workflow with a rule step you receive a message that the solution cannot be validated because no definition was found for the ICM_RuleOperations queue.

Symptoms

In a production environment, you try to copy a solution that contains a workflow with a rule step by using the IBM Case Manager administration client and you receive an error message such as the following message:

```
The original solution could not be validated. See the following error:
FNRPA0276e: The XPDL document for the original solution could not be
validated because of the following error: SM032_T1:Rule Step1:[ERROR]
Definition not found for Queue: "ICM_RuleOperations". (ICM_RuleOperations)
SM032_T1:Rule Step1:[ERROR] Execute instruction uses operation,
executeRule, which is not defined for queue ICM_RuleOperations.
```

Causes

The validation errors prevent you from copying the solution.

Resolving the problem

When you copy the solution in the IBM Case Manager administration client, select the **Skip validation** check box.

Cannot deploy a solution with business rules if transaction timeout value is too low

You cannot deploy a solution that contains business rules if the transaction timeout setting of the application server for Content Platform Engine is too low.

Symptoms

When you deploy a solution that contains rules, the following error message is returned:

```
FNRPA0624E The rules could not be deployed because of the following error:
A transaction problem has occurred. Message was: ; nested exception is:
com.ibm.websphere.csi.CSITransactionRolledbackException: Transaction marked
rollbackonly 7/19/13 11:14:06 PM PDT FNRPA0093E The previous error was
caused by: A transaction problem has occurred. Message was: ; nested
exception is: com.ibm.websphere.csi.CSITransactionRolledbackException:
Transaction marked rollbackonly
```

Causes

The transaction timeout setting of the application server for Content Platform Engine is too low.

Resolving the problem

If you encounter this problem, temporarily set the value of the transaction timeout setting to a higher value:

- If Content Platform Engine runs on WebSphere Application Server, go to the **Application servers** > **server1** > **Transaction service** page in the WebSphere Application Server administrative console and increase the value of the **Total transaction lifetime timeout** setting to a higher value, such as 300 seconds.
- If Content Platform Engine runs on Oracle WebLogic Server, open the WebLogic Server Console and go to the JTA Configuration page for the domain in which Content Platform Engine is installed. Change the value of the **Timeout Seconds** field.

After the solution is successfully deployed, change the value of the transaction timeout setting back to the previous value.

Rule steps do not run if processing timeout value is too low

Rule steps might not run if the processing timeout value for the rules component queue is too low.

Symptoms

In Case Manager Client, you view the details of the task that contains the rule step and see that the task failed with the error `Work Performer Exception:null`. In addition, the following error message is written to the `pesvr_system.log` file during rule execution:

```
CMExecute[1].int2vm13cmtosuser.FNTARGETDS_1 .ICM_RuleOperations.P8Admin [
LOAN1_PoorCreditRating: 93A2C03B20B4314BA02B16087B5BFC3C:Workflow:
executeRule] FAILED.; Exception: java.lang.InterruptedException
at java.lang.Object.wait(Native Method)
at java.lang.Object.wait(Object.java:485)
at ilog.rules.res.xu.ruleset.internal.IlrRulesetProvider.getRuleset
(IlrRulesetProvider.java:213)
at ilog.rules.res.xu.spi.IlrManagedXUConnection.createEngineManager
(IlrManagedXUConnection.java:1443)
at ilog.rules.res.xu.spi.IlrManagedXUConnection.getEngineManager
(IlrManagedXUConnection.java:1319)
at
ilog.rules.res.xu.spi.IlrManagedXUConnection.getXURulesetArchiveInformation
(IlrManagedXUConnection.java:1260)
```

```
at ilog.rules.res.xu.cci.IlrXUConnection.getXURulesetArchiveInformation
(IlrXUConnection.java:466)
at ilog.rules.res.xu.cci.IlrXUInteraction.getRulesetInformation
(IlrXUInteraction.java:561)
at ilog.rules.res.xu.cci.IlrXUInteraction.dispatchExecution
(IlrXUInteraction.java:129)
at
ilog.rules.res.xu.cci.IlrXUInteraction.execute(IlrXUInteraction.java:253)
```

Causes

The process timeout setting for the ICM_RuleComponent queue is too low.

Resolving the problem

If you encounter this problem, set the processing timeout value for the rules component queue to a higher value, such as 120000 milliseconds (2 minutes). You might need to set a higher value depending on the workload of Content Platform Engine. By default, the timeout value is 60000 milliseconds.

To set the processing timeout value for the rules component queue:

1. In Process Configuration Console, select the appropriate connection point.
2. Click **Component Queues** > **ICM_RuleOperations**.
3. In the Component Properties window, click the **Adapter** tab and modify the value of the **Processing Timeout (ms)** field.

Tip: When you migrate a solution that contains business rules to another development or production environment, use the rules component processing timeout setting in the source environment as a guideline when you set the rules component processing timeout setting in the target environment. However, you might be able to use lower timeout values when you migrate from development to production environments because production environments are typically faster than development environments. After you adjust the timeout value, ensure that you test the system to ensure that the adjusted value is appropriate for the system.

Troubleshooting business rule errors

You might receive errors that are related to business rules when you deploy or run IBM Case Manager.

Symptoms

You receive errors that are related to business rules when you deploy or run IBM Case Manager.

Resolving the problem

To troubleshoot any errors that occur during deployment that might be due to business rules:

1. Determine which business rules are the source of the problem by checking the IBM Case Manager deployment log in Case Manager Builder. Alternatively, you can validate each case type. For more details about the errors, see the Content Platform Engine server logs.
2. Open each of the problematic business rules in the rules designer in Case Manager Builder and fix any errors that are listed.

To troubleshoot any errors that might be due to business rules when you run IBM Case Manager, check the messages in the Content Platform Engine server logs. You can view all information and trace messages from the rule operations component

in the Content Platform Engine trace log file (pesvr_trace.log) if the TRACE_CM trace option is enabled for Content Platform Engine. For information about configuring the Content Platform Engine trace log file options, see the trace topic in the IBM FileNet P8 documentation.

Tip: You can specify one or more print actions in a rule so that the associated rule step returns the specified strings to the workflow in the return_value data field. The return value of the rule step can then be mapped to a data field that can be used by the next step in the workflow. The print statements are also included in the Content Platform Engine trace log if the TRACE_CM trace option is enabled for Content Platform Engine.

Troubleshooting case history table lock escalation errors

If table lock escalation errors occur when case history data is processed, you can bypass new errors by increasing the size of the log file for the case history database and increasing the maximum number of table locks.

Symptoms

Errors occur during case history processing, such as an error that indicates that the tablespace of the case history database is full. Over time, many events accumulate until the error is solved. As a result, you might see "active log is full" errors and table lock escalation errors.

Resolving the problem

To bypass new errors so that table deadlock does not occur until the original problem is solved, increase the size of the log file and lock list for the case history database. For example, enter the following commands:

```
db2 update db cfg using MAXLOCKS 100
db2 update db cfg using LOCKLIST 8192
```

Database deadlock issue with large solution deployments

When you try to deploy a large solution, a database deadlock error might be generated in the IBM FileNet P8 server error log.

Symptoms

You try to deploy a large solution and a database deadlock error is generated in the IBM FileNet P8 server error log, such as the following error:

```
013-07-12T16:48:33.293 19F319F3 ENG FNRCE0019E - ERROR method name:
throwEngineException principal name: Administrator Global Transaction: true
User Transaction: false Exception Info: The operation could not be
completed due to a deadlock error. A retry might be appropriate.
ObjectStore: "CMTOS", SQL: ""ALTER TABLE CMTOS.Container ADD
(u2586_dub_hvlointeger67 number(10) NULL) ""
com.filenet.api.exception.EngineRuntimeException: FNRCE0019E:
E_DEADLOCK_ERROR: The operation could not be completed due to a deadlock
error. A retry might be appropriate. ObjectStore: "CMTOS", SQL: ""ALTER
TABLE CMTOS.Container ADD (u2586_dub_hvlointeger67 number(10) NULL) ""
failedBatchItem=42
at com.filenet.engine.dbpersist.DBOracleContext.throwEngineException
(DBOracleContext.java:335)
at com.filenet.engine.dbpersist.DBExecutionElement.execute
(DBExecutionElement.java:296)
at com.filenet.engine.dbpersist.DBExecutionContext.getNextResult
(DBExecutionContext.java:106)
```

```
at com.filenet.engine.dbpersist.DBStatementList.executeStatements
(DBStatementList.java:161)
at com.filenet.engine.dbpersist.DBStatementList.getNextResult
(DBStatementList.java:601)
at com.filenet.engine.dbpersist.DBStatementAlter.process
(DBStatementAlter.java:834)
at com.filenet.engine.dbpersist.DBStatementAlter.process
(DBStatementAlter.java:778)
```

Causes

The system determines whether a solution is active by periodically checking the LastModified time of the solution folder. A keep-alive interval specifies how often solution activity is checked. The default keep-alive interval of 2 seconds is too small for large solution deployments.

Resolving the problem

For large solution deployments, increase the value of the keep-alive interval from 2 seconds to 30 seconds. The value is specified in milliseconds: 30000 is 30 seconds.

To increase the keep-alive interval to 30 seconds:

1. Set the following JVM parameter on the IBM Case Manager server:
   `-Dcom.ibm.casemgmt.config.keep.alive.interval=30000`
2. Restart the JVM for your changes to take effect.

Event payloads can contain model objects that are not fully retrieved

Event payloads can sometimes contain sparse model objects that are not fully retrieved.

Symptoms

Event payloads can sometimes contain sparse model objects that are not fully retrieved. Performing operation on these model objects by invoking APIs will return null values.

Resolving the problem

If this problem occurs, refer to the JavaScript API documentation for that model class and use the correct APIs to completely retrieve the model object.

Improve performance at case creation time by limiting subfolder structure

To improve performance at case creation time, limit the predefined subfolder structure in your case design to 10 or fewer subfolders. The more subfolders that are in a predefined subfolder structure, the longer case creation can take. To reduce the time that it takes to create a case, limit the complexity of your predefined folder structure.

For example, you might design a case with up to 10 subfolders directly under the case. As another example, you might design a case with two subfolders directly under the case and with four subfolders under each of the higher-level subfolders. Various other combinations might also yield a predefined subfolder structure of 10 or fewer subfolders.

If your solution requires cases with a more complex subfolder structure, create the folders after the case is initialized. You can add them programmatically, within an automatic task process, or allow users to add them on demand as needed.

IBM Case Manager administration client does not remove all files that are related to the package

To completely remove a custom widgets package, you must manually delete some additional files after you use the administration client to delete the package.

When you use the administration client to delete a custom widgets package, the package is removed from the following locations:

- In IBM Content Navigator: **design_object_store** > **root** > **IBM Case Manager** > **widgets**
- In the Case Manager installation: `/install_path/IBM/CaseManagement/configure/properties/widgetsPackage/design_object_store`

However, two other locations still contain artifacts from the package. You can clean up the remaining artifacts by manually deleting them.

- In the IBM Content Navigator plug-ins list, delete the plug-in for the custom widget package.
- In the IBM Case Manager installation, delete the plug-in for the custom widget package from the plug-ins directory.

  Important: The following path is the default location. Your plug-ins directory might be in a different location. `/install_path/IBM/CaseManagement/configure/properties/plugins`

Supporting external documents in production environments

To support external documents in a production environment, you must update security settings in the Administration Console for Content Platform Engine.

About this task

In a production environment, users cannot add external documents into case folders because the default instance security settings of the External Document class are removed incorrectly.

To work around this issue, manually configure the default instance security settings of the External Document class:

Procedure

1. In the Administration Console for Content Platform Engine, open your target object store and click **Data Design** > **Classes** > **Document** > **External Document**.
2. On the Default Instance Security tab, add an entry with the name `#CREATOR-OWNER` and assign it the View properties permission. Also, ensure that the **Default Instance Owner** field is set to `#CREATOR-OWNER`.

Older versions of an audit or security configuration in the IBM Case Manager administration client might not be re-imported

You cannot roll back an audit or security configuration to an older version by using the IBM Case Manager administration client to re-import the older configuration if a newer configuration exists in the same environment.

You can use the IBM Case Manager administration client to import an audit or security configuration that you created on another object store. For example, you might create a security configuration in your development environment, export that configuration, and then import that configuration to your production environment.

If you then change the security configuration in your production environment, that newer version becomes different from the version that you imported from your development environment. However, the names of the security configurations in both environments remain the same.

If you subsequently decide that you want to roll back the changes that you made to the security configuration in your production environment and you attempt to re-import the security configuration from your development environment, the production security configuration is not overwritten. This result occurs because the security configuration in your development environment has the same file name as the security configuration in your production environment, but the development version is older than the production version. The IBM Case Manager administration client does not overwrite a newer configuration with an older configuration of the same name.

To roll back the changes that you made to the security configuration in your production environment, first delete the changed configuration from the production environment. Then, export the security configuration from your development environment and re-import it to your production environment. The IBM Case Manager administration client does re-import the security configuration if a newer configuration of the same name does not already exist in the production environment.

Related tasks

"Importing the audit configuration" on page 155

"Importing the security configuration" on page 154

EAR file for custom widget package isn't deployed

You can use the IBM Case Manager administration client to register a custom widget package.

Symptoms

If the package contains an EAR file, the EAR file isn't deployed.

Resolving the problem

If a custom widget package contains an EAR file, use the IBM Case Manager configuration tool to deploy and register the package.

Important: If you run the Deploy and Register Widgets Package task in a cluster environment, you must ensure that the plug-in is loaded on each node of the

cluster. Either restart the cluster to force the plug-in to be loaded on all nodes or manually load the plug-in on each node by using the IBM Content Navigator administration client.

Alternatively, register the package by using the IBM Case Manager administration client and then manually deploy the EAR file.

1. Register the custom widget package:
   a. Extract the files in the package compressed file to a directory on the IBM Case Manager server. For example, extract the files to a temporary directory.
   b. Log in to the IBM Case Manager administration client on the server where IBM Case Manager is running.
   c. Point your browser to `https://server:port/navigator/?desktop=icmadmin` where *server* is the host name or IP address of the IBM Case Manager server and *port* is the IBM Content Navigator port number.
   d. Navigate to **Object Stores** > **Design Object Store** > **Widget Packages**.
   e. Select **Import Custom Widget** and then browse to find the package compressed file.
   f. Complete the wizard steps.
2. Manually deploy the EAR file:
   a. Log in to the IBM WebSphere Application Server administrative console.
   b. Point your browser to `https://server:port/ibm/console` where *server* is the host name or IP address of the IBM Case Manager server and *port* is the IBM Content Navigator port number.
   c. Install the EAR application from the custom widget package:
      1) Navigate to **Applications** > **Application Types** > **WebSphere enterprise applications**.
      2) From the Enterprise Applications page, click **Install**.
      3) From the "Preparing for the application installation" page, select **Local file system** and then select the local package compressed file.
      4) Complete the wizard steps.
      5) Start the EAR application by navigating to **Applications** > **Application Types** > **WebSphere enterprise applications**, selecting the EAR application, and clicking **Start**.

IBM Case Manager configuration tool task fails with 414 error

Running the Register Target Environment configuration task in an environment with Oracle HTTP Server results in a 414 Request-URI Too Large error.

Symptoms

The following error is displayed on the console for the Register Target Environment configuration task:

```
An error occurred while running New_Register Target Environment
The task failed because of the following error:
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>414 Request-URI Too Large</title>
<head><body>
<h1>Request-URI Too Large</h1>
<p>The request could not be processed by the server. The request URI
is longer than the permissible limit.</p>
</body></html>
```

Causes
The size of the HTTP request line is larger than 8190 bytes.

Resolving the problem
To resolve the problem:

1. Increase the size of the HTTP request line that is accepted from a client by updating the `httpd.conf` file for Oracle HTTP server to contain the following line:

   ```
   LimitRequestLine 16384
   ```

   For complete information about the LimitRequestLine parameter, see the "LimitRequestLine Directive" section of the Oracle documenation at http://docs.oracle.com/cd/B14099_19/web.1012/q20206/mod/core.html.
2. Restart Oracle HTTP Server.

Re-creating an IBM Case Manager target object store in a development environment

If the development target object store for IBM Case Manager is corrupted or unusable, you can re-create it.

Symptoms
The target object store might become corrupted or left in an uncertain state during development activities.

Resolving the problem

To recover the target object store, you must re-create its metadata and standard environment. As a result, runtime data, such as cases and documents, is lost. To re-create the object store, you must be a system administrator and be familiar with the following concepts:

- IBM Administration Console for Content Platform Engine
- General installation steps for IBM Case Manager
- General installation and administration skills for the Content Platform Engine, IBM Case Manager, and integrating components that are configured on your system (such as Case History, Case Analyzer)

To re-create the IBM Case Manager target object store, follow this procedure:

1. Back up your design object store database.
2. Use IBM FileNet Deployment Manager to export the external solutions artifacts you want to keep. For more information, see Saving user-defined assets before you reset the test environment.
3. Note the properties of the target object store and the other components of the content management system that reference it. You need these property values to clean up resources and re-create components. For example, the following properties are important:
   - The names of servers, database instances, and database schemas.
   - The names of database connections and data sources.
   - Storage locations for tables, indexes, and large objects (LOBs) for the target object store and workflow system data.

- For the target object store, note the symbolic name, the user groups to which you grant administrative and basic access, the project area name, the IBM Content Navigator desktop name, and the case operations user name and password;
- Any add-ons that are added to the target object store. To determine the add-ons, log in to IBM Administration Console for Content Platform Engine, navigate to the target object store, click **Actions**, then click **Install Add-on Features**. Note what add-ons are in the Installed add-on features list, then click **Cancel**.
- For workflow systems, note the default locale, date/time mask, XSL/XSD base directory, workflow system administration and configuration groups, process orchestration broker servlet URL, public listener URLs, connection point name, and isolated region name.
- For Case Analyzer stores, note the event pruning schedule and publishing interval.

4. Set the application server timeout values to at least 600 seconds. The following sample settings are for IBM WebSphere Application Server Version 8.5.2:
   - **Servers** > **Server Types** > **WebSphere application servers** > **Configuration tab** > **Container Settings** > **Container Services** > **Transaction service** > **Total transaction lifetime timeout**
   - **Servers** > **Server Types** > **WebSphere application servers** > **Configuration tab** > **Container Settings** > **Container Services** > **Transaction service** > **Maximum transaction lifetime timeout**
   - **Servers** > **Server Types** > **WebSphere application servers** > **Configuration tab** > **Container Settings** > **Container Services** > **ORB service** > **Request timeout**
   - **Servers** > **Server Types** > **WebSphere application servers** > **Configuration tab** > **Container Settings** > **Container Services** > **ORB service** > **Locate request timeout**

     Note: For WebSphere Application Server Version 8.5.2, the maximum value for the locate request timeout is 300.
   - **Resources** > **JDBC** > **Data sources** > **[Content Engine or Case Manager data source name]** > **Connection Pool properties** > **Connection timeout**
   - **Resources** > **JDBC** > **Data sources** > **[Content Engine or Case Manager XA data source name]** > **Connection Pool properties** > **Connection timeout**
5. If the Content Platform Engine is running in an application server cluster, stop all but one of the nodes.
6. In IBM Administration Console for Content Platform Engine, first delete all components that reference the target object store, including the connection points and workflow systems, then delete the target object store. For information, see Deleting an object store.

   Note the following information:
   - The Deleting an object store topic does not provide a complete list of all of the integrating components that can reference an object store, such as Case Analyzer stores. If components exist that reference the target object store, those components must be deleted before you can delete the target object store.
   - When you delete the case history store, you might get an error similar to the following error:

```
The case history store could not be deleted because of the following error:
com.filenet.api.exception.EngineRuntimeException: FNCRE0066E:
E_UNEXPECTED_EXCEPTION: An unexpected exception occurred. The unexpected
exception is chained to this exception. Message was: null FNRAM9022
```

In this error occurs, log in to IBM Administration Console for Content Platform Engine, then navigate to **[ECM Domain Name]** > **Global Configuration** > **Administration** > **Database Connections** > **[target object store database connection]** . On the **Properties** tab, scroll to the Event Export Stores property. Verify that this value does not reference an event export store. The property value must be either `Event Export Stores`, or `<No items found>`.

7. In IBM Administration Console for Content Platform Engine, perform the following tasks:
   - Navigate to the connection definition in the design object store that is associated with the target object store: **Object Stores** > **[design object store name]** > **BrowseRoot Folder** > **IBM Case Manager** > **Datasets** > **DevEnvReinitInfo** > **[connection definition name]**.
   - Delete all the documents except DeployDataset. Do not change the DeployDataset document. Delete the following documents (if they exist): CodeModules, DevEnvReinitManifest, DevEnvReinitStatus.
8. Log out of IBM Administration Console for Content Platform Engine, then stop IBM FileNet Enterprise Manager and any custom applications that might be accessing the target object store.
9. Stop the last Content Platform Engine node.
10. For each of the deleted components that use a database, log in to the database administration console and delete all the user tables in their schemas, leaving the system tables only. These components include the workflow system and target object store. If any other deleted components have database tables, delete those tables as well. For example, the Case Analyzer store is a component that has database tables.

    Note: After you delete the target object store tables, you must also delete the sequences associated with the target object store database schema. For more information, see Deleting an object store
11. Start the Content Platform Engine. In a clustered environment, start all the nodes.
12. To add an target object, log in to IBM Administration Console for Content Platform Engine, navigate to the Object Stores node, and click **New** store.
    - Use the same symbolic name as the original target object store.
    - Reuse the database connection and schema of the original target object store.
    - The user group that you grant administrative access to must have Full Control access. The new target object accesses the connection definition that is associated with the project area. The user group that you grant basic access to must have View properties access to the connection definition.
    - In the **Select Add-ons** window, click **Workplace/WorkplaceXT Configuration**. Do not select any more add-ons.
13. In IBM Administration Console for Content Platform Engine, navigate to the connection definition **Security** tab:
    a. **Object Stores** > **[target object store name]** > **Browse** > **Root Folder** > **IBM Case Manager** > **Datasets** > **DevEnvReinitInfo** > **[connection definition name]** > **Security**

b. Verify that the target object store administrative and general (basic access) user groups have security access (as described in the previous step). The user group that you grant administrative access to must have Full Control. This object accesses only the connection definition associated with the project area. The user group that you grant basic access to must have View properties access to the connection definition.

14. In IBM Administration Console for Content Platform Engine, navigate to **Object Stores** > **[target object store name]** > **Administrative** > **Workflow System**. Click **New** to add a workflow system.

    Note: You can reuse the same properties in the original workflow system, such as the database storage locations (tables, index, LOB), connection point name, and region name.
15. Log out of IBM Administration Console for Content Platform Engine and start the Case Manager Configuration Tool. Open your profile, then open the profile properties and test the server connections.
16. Run the following tasks in the Case Manager Configuration Tool. Use the original parameter values that you noted before the object store was deleted:
    a. Configure the Case Management Object Stores. This step adds the target object store and analytics add-ons.
    b. Register Project Area
    c. Configure Business Rules
17. In IBM Administration Console for Content Platform Engine, add any add-ons from the original target object store that still need to be added.
18. Log in to Case Manager Builder and deploy your solutions.
19. Use FileNet Deployment Manager to import external solution artifacts that you want to keep.
20. Re-create any other integrating components that were deleted.

Configure Box Collaboration task fails in a distributed environment when the date/time is not synchronized

In a distributed or cluster environment, the Configure Box Collaboration task does not run if system time is not synchronized with the internet time.

Symptoms

You attempt to run the Configure Box Collaboration task from either the IBM Case Manager administration client or the IBM Case Manager configuration tool. However, the task fails to run and returns error FNRPA0791E that states that the current date/time is later than the expiration date/time in the “exp” claim.

Resolving the problem

Synchronize the system time on your IBM Case Manager server with the internet time. For instructions on synchronizing the time, refer to the operating system documentation.

Troubleshooting Case Manager Builder

Troubleshoot typical errors that might surface in the Case Manager Builder.

Tip: To run Case Manager Builder in debug mode, add the `debug=true` flag to the Case Manager Builder URL as shown in the following example:

```
http://localhost:9080/CaseBuilder?debug=true
```

Changing the screen display resolution for Case Manager Client and Case Manager Builder

The default screen size for Case Manager Client and Case Manager Builder can be too large for small computer monitors with low resolution (for example, 768x1080).

Symptoms

A scroll bar is displayed at the bottom of the screen.

Causes

The default screen resolution assumes larger computer monitors with large screen resolution settings. Smaller computer monitors with low resolution require a horizontal scroll bar to view the entire application.

Resolving the problem

Press Ctrl+minus sign key (-) to fit the entire application on a low resolution screen without the horizontal scroll bar.

Note: This workaround does not change the configured screen resolution; it changes the size of the application within the browser.

Solution deployment fails due to a queue table limit

Deploying a solution from Case Manager Builder to the development target object store fails due to a database limitation.

Symptoms

You use Case Manager Builder to deploy a solution, and receive an error message similar to the following message:

```
12/6/10 12:35:21 PM PST FNRPA0032E The solution cannot be deployed because
the Process Engine configuration document could not be found. See the following
error: Too many user defined fields in queue table (limit of 220?), table
name=DefaultWPCTable
```

Causes

The case management database has a limit of 220 columns per queue, and there is one queue for each role in-basket. Each property that you add to a case requires a column in the database. If you deploy multiple solutions with large numbers of properties to your test environment, you can exceed the column limit.

Once you reach the limit and receive the FNRPA0032E error message, you must reset the test environment to clear the tables. Resetting the test environment removes all of your deployed solutions and other data from the development target environment and reinitializes the isolated region.

Resolving the problem

To reset the test environment:

- In Case Manager Builder, click **Actions** > **Reset Test Environment** on the Manage Solutions page.

  Note: Resetting the test environment removes all the data from the development target environment, including any FileNet P8 assets that you copied from your production environment and any assets you created outside of Case Manager Builder to extend the solution design, such as search templates or form templates.

Responding to validation errors in the Step Designer

If you receive a validation error message when you validate a task in the Case Manager Builder Step Designer, you must confirm that roles and properties that are referenced in the Step Designer are valid for the solution and confirm that your routes meet the validation guidelines. You might also see errors when you open a Task in the Step Designer.

Symptoms

You receive an error message like the following errors:

```
FNRPB6202E: An error occurred during validation.

FNRPB1005E: A network operation was stopped while trying to complete
 the Load Task action.
```

The FNRPB6202E error always includes an associated error message. One of the following messages might be displayed:

```
Step: [ ERROR ] Step cannot be reached from the launch step.

Step: [ ERROR ] No and-join step found for and-split step

: [ ERROR ] Route from Step to Step is incorrectly nested.
```

```
WFC: [ ERROR ] WaitForCondition instruction references work
class, ACM-SalaryInfo, but no work class of that name
was found with the transfer flag set in the workflow collection
or on the server.

WFC: [ WARNING ] WaitForCondition instruction references work
class, ACM-class_name, but no work class of that name
was found with the transfer flag set in the workflow collection.
Using the definition previously transferred to the server.

WFC 2: [ ERROR ] WaitForCondition instruction references work
class, ACM-class_name, but no work class of that name
was found with the transfer flag set in the workflow collection
or on the server.

WFC 2: [ WARNING ] WaitForCondition instruction references work
class, ACM-class_name, but no work class of that name
was found with the transfer flag set in the workflow collection.
Using the definition previously transferred to the server.
```

Causes

Validation errors might be caused by the following actions:

- Editing or deleting a role or property that is used in the task from the solution. If you save the solution and then later edit or remove a role or property that is used in a Task, you receive a validation error when you validate the task again in the Step Designer.

  Restriction: For best results, do not edit or remove a role or property that is used in a solution until after you edit the Task in the Step Designer.
- Creating a step that cannot be reached.
- Defining a step as an AND-split without defining a step as the AND-join.
- Creating routes that are invalid.
- Creating a task that is dependent on another XPDL file.

Resolving the problem

To resolve the validation error:

1. Click the **error text** in the status bar to view the associated message.
2. Complete one of the following steps to resolve the problem:

- If you must edit or delete a role or property that is used in the task, first edit the task in the Step Designer to remove the property or role. Then, edit the role or property at the solution level. Open the task again in the Step Designer if you must use the modified role or property.
- Ensure that each step in the map can be reached.
- Define an AND-join step for each AND-split step.
- Ensure that the connectors and steps that you defined meet the requirements for valid workflow routes.
- If your workflow includes a step that is dependent on a step in another XPDL file, then open the workflow in Process Editor and run the validation there. If the WCF errors in the Step Designer are warnings in the Process Editor instead of errors, you can ignore the errors in the Step Designer. Otherwise, use the Process Editor validation correction feature to correct the problem.

Reviewing log entries in Case Manager Builder

Case Manager Builder displays error messages and status messages in the status pane at the bottom of the window when the error or status update occurs. You also can view the entire contents of the log file in the status pane, or you can view only the errors from the log.

Symptoms

You want to view the entire content of the log file for a solution instead the most recent single message, or you want to view only the error entries from the log file.

Resolving the problem

To view the log file:

- From the Manage Solutions page, click **More Actions** > **Logs** for the solution for which you want to review the log entries. The log entries are displayed in the status pane at the bottom of the page.

To view only the errors from the log file:

- From the Manage Solutions page, click **More Actions** > **Errors** for the solution for which you want to review the error entries. The error entries from the log file are displayed in the status pane at the bottom of the page.

Tip: You can copy the text from the status pane and paste it into word processor or other file for additional review.

Cannot edit locked solution assets

A solution asset is locked when another user opens the asset for editing and does not commit the solution properly, or a session times out, which can prevent other users from editing the asset.

Symptoms

A solution asset is locked and you cannot edit it.

Causes

A solution asset can be locked in the following situations:

- Another user opens the solution asset in Case Manager Builder and closes the browser without committing the solution.
- Another user opens the solution asset in Case Manager Builder and the session times out.
- Another user opens the solution asset in Process Designer and closes Process Designer without committing the solution in Case Manager Builder.

Diagnosing the problem

If you open a solution asset in Case Manager Builder and do not commit the solution properly, or if the session times out, you can still open and edit the asset. If you create or edit a solution by using Case Manager Builder, commit the solution, and then cannot open and edit an asset, the solution asset might be locked because another user did not commit the asset properly, the session timed out, or the other user is still editing the asset.

Resolving the problem

Determine who is editing the asset by clicking **Show Locked Items**, and then ask the user to commit the solution to unlock the asset. If the user cannot commit the

solution, for example the user is on vacation or left the company, ask your system administrator to unlock the asset by using the IBM Case Manager administration client.

Attention: When an asset is unlocked by using the IBM Case Manager administration client, any draft edits that were made to the asset are lost.

Related concepts

Multiple user editing of solutions

Related tasks

"Unlocking solution assets" on page 37

Case type validation errors

If you receive an error message when you validate a case type in the Case Manager Builder, you must ensure that you saved the solution first.

Symptoms

You receive one of the following messages:

An error occurred while using the Process Engine API. (FNRPB4066E)
: This message occurs after you create a solution in Case Manager Builder, add a case type or an IBM Business Process Manager task, and click the **Validate** button to validate the case type.

The required process application and snapshot information is missing from the solution. (FNRPB6111E)
: This message occurs after you add a solution in Case Manager Builder, click save, add a case type, add a IBM Business Process Manager task, and click the **Validate** button to validate the case type.

Causes

The case type validation errors are caused by one of the following reasons:

- Case Manager Builder does not create a Global XPDL file until the first save of the solution. Therefore, case type validation fails.
- Case Manager Builder does not keep the IBM Business Process Manager information until the solution is saved for the first time. Therefore, Case Manager Builder cannot find the IBM Business Process Manager information to validate the IBM Business Process Manager task.

Resolving the problem

You must save a new solution before you can validate it.

Cannot reset the test environment because target object server does not exist

Resetting the test environment fails because the target object server does not exist.

Symptoms

You attempt to reset the test environment, and receive an error message similar to the following message:

```
FNRPA001E Data cannot be retrieved from the connection definition because the
following error occurred: The requested item was not found. Non-repository
object {91DC01CE-B104-42B6-9CooA-EEE9F62731DB2} not found.
```

Causes

The target object store was accidentally removed or it is corrupt.

Resolving the problem

If you have a valid manifest, you can recreate the target object store. To recreate the target object store complete the following steps:

1. In the Firefox browser, download the Post plugin.
2. In the Post plugin window, enter the information for your target object server and click **Post**.

Deploy dataset not found when the test environment is reset

You cannot reset the test environment because the FileNet Deployment Manager deploy dataset is not found.

Symptoms

When you try to reset the test environment, you receive an error message similar to the following message: `FNRPA0403I No DataSet object can be found for the FileNet Deployment Manager import operation.`

Resolving the problem

To resolve the problem:

1. Verify that the `deployDataSet1.xml` file is in the content element list for the DeployDataset document.
   a. In IBM Administration Console for Content Platform Engine, select the case management design object store.
   b. Click **Browse** > **Root Folder** > **IBM Case Manager** > **Datasets** > **DevEnvReinitInfo** > **dev_env_connection_definition**.
   c. On the dev_env_connection_definition page, click **DeployDataset** in the **Containment Name** column.
   d. On the DeployDataset page, click the **Content Elements** tab and verify that the `deployDataSet1.xml` file is listed.
   e. If the `deployDataSet1.xml` file is not listed, you must add it to the DeployDataset document.
      1) Click **Actions** > **Checkin, checkout, cancel** > **Exclusive checkout**, and then click **Actions** > **Checkin, checkout, cancel** > **Checkin**.
      2) In the Checkin Document window, click **Add** to navigate to the deploy dataset folder and attach the `deployDataSet1.xml` file.
      3) Click **Checkin**.
2. Ensure that the application server administrative user has full control privileges for the temporary directory in which the dataset content is saved. To determine the path to the temporary directory, look in the Case Manager Builder status pane for a message such as `FNRPA0439I The data set content is being saved to C:\Windows\TEMP\`.

Document opens in another window even when the Viewer widget is present

A default setting in Case Manager Builder can cause unexpected behavior when you view documents or attachments on the Case Details page.

Symptoms

You open a document on a Case Details page that includes the Viewer widget and you expect to see the document displayed in the Viewer widget. Instead, the document opens in a new window.

Causes

The **Open document in a separate browser window** checkbox on the Case Details page in Page Designer is checked by default. The result is that even if you add a Viewer widget to the page, the page will still open a new window to display a document or attachment.

Resolving the problem

To overcome this problem:

1. Open your Case Details page in Page Designer.
2. Add the Viewer widget to the page.
3. In the settings for the Case Information widget on this page, clear the **Open document in a separate browser window** checkbox.

Toolbar buttons on Rules and Tasks pages are not displayed in Internet Explorer

When you view Case Manager Builder in Internet Explorer 8, you cannot see the toolbar buttons on the Rules and Tasks pages.

Symptoms

You run Case Manager Builder in Internet Explorer 8 and open the Rules or Tasks page. You cannot see the toolbar buttons.

Causes

The Microsoft Silverlight add-on in Internet Explorer 8 might prevent the toolbar buttons in Rules and Tasks pages from being displayed.

Resolving the problem

To overcome this problem, disable the Microsoft Silverlight add-on:

1. In Internet Explorer, click **Tools** > **Manage add-ons** and click **Toolbars and Extensions**.
2. Disable Microsoft Silverlight.

Cannot add a column to display the case type for a work item in an in-basket

You cannot add case type as a property in an in-basket in Case Manager Builder. You must use Process Designer to configure an in-basket to display case types.

Symptoms

The case type is not included as an option in the **Select Properties** list when you edit an in-basket in Case Manager Builder.

Resolving the problem

You can configure an in-basket to display a column for case types by using Process Designer.

To configure an in-basket to display a column for case types:

1. On the Manage Solutions page in Case Manager Builder, click **More Actions** > **Open Process Designer** for your solution.
2. In the Case Type Selection window, select any case type from your solution and click **OK**.
3. Click **View** > **Configuration**.
4. Expand **Work Queues**, right-click the role queue for which the in-basket is used, and click **Properties**.
5. Click the **In-baskets** tab and add case types as a column:
   a. Click the **Add** icon and select **CmAcmCaseTypeID (Guid)** in the **Available Fields** list. Then, click **OK**.
   b. Change the label for the column.

      Important: Do not enable the case type column for sorting. If you do enable sorting, the results are inconsistent because sorting is sometimes done in the browser and sometimes on the server. Sorting on the server uses the internal names of the case types. Sorting in the browser uses the display names of the case types.
   c. Click **OK** > **File** > **Solution** > **Save And Close**.
6. In Case Manager Builder, commit your changes.

Columns overlap when column dimensions are set too large in the page designer

When designing a page, the columns may overlap if the settings for the width or height exceed the page design area.

Symptoms

If you set the dimensions (width and height) of a column to exceed the page editor area with multiple columns, the columns may overlap, and functionality in the columns may be inaccessible.

Causes

The columns may be overlapping if you have entered a value or values for the dimensions of one or more columns in the Page Options window that is too large for the columns on the page. The value may be too large because:

- You inadvertently entered a large value for a height or width value for the page layout.
- You have entered values that are correct for your design requirements, but are too large for the browser or monitor you are using.

Resolving the problem

If the values entered for the width or height are not correct, you can change them to the correct values in the Page Options window. If the values are correct and fit your requirements, you may need to enlarge your browser window or use a larger monitor to design the page.

Troubleshooting overlap and gap warnings in table-based rules

When you edit table-based business rules, you might receive overlap and gap warnings.

Symptoms

Orange icons are displayed in the lower left corners of cells in the table-based business rule.

Causes

Warnings are displayed in table-based rules for the following reasons:

Overlaps
When two cells in a column contain ranges that include the same values. For example, the ranges `[200,000; 300,000]` and `[200,000; 600,000]` both include the numbers 200,000 - 300,000.

Gaps When two cells in a column contain ranges that do not include values between the ranges. For example, the ranges `< 100,000` and `[200,000; 600,000]` do not cover the numbers 100,000 - 200,000.

Resolving the problem

Because overlaps and gaps do not prevent a rule from running, you can deploy a rule that has gap and overlap warnings. However, overlaps and gaps might produce incorrect results when the rule runs if there are ambiguities in the rule definition.

By default, rule designer checks for overlaps and gaps in all columns. If you do not want rule designer to display gap and overlap warnings for a particular column, right-click the header cell of the column and clear the **Check Gap** and **Check Overlap** check boxes.

In some cases, empty rows are considered as gaps and are flagged with warnings. To resolve these warnings, click the optimize icon in the upper left corner of the table-based rule to remove any empty rows and arrange the data in ascending order based on the values in the first column. The optimize icon is enabled only after you make changes to the table-based rule.

To resolve gaps in a particular column, you can add a row with the value **Otherwise** to define a rule to use in case none of the other values for the condition in that column are true. To set the value of a cell to **Otherwise**, right-click the cell and click **Set to Otherwise**.

Related tasks

Checking errors and warnings

Cannot view values when you edit cells in table-based rules

When you type values in the cells of a table-based business rule, you cannot see the values until you press Enter.

Symptoms

When you click in a cell of a table-based business rule, you cannot see the values as you type or edit them until you press Enter.

Causes

The editing area in the cell is small by default.

Resolving the problem

To work around this problem, try to expand the cell so that you can view the entire typing area. Alternatively, you can edit the value by right-clicking a cell and clicking **Edit Custom Value**.

Related tasks

Editing cells

Comments in scripts cause a validation error

If you enter a comment in the script for a script action or in the Script Adapter widget, Case Manager Builder might return a validation error.

Symptoms

You create a script that is run from the Script Adapter widget or from a script action in a toolbar or menu. In the script, you add a comment that starts with two forward slashes. If the comment is in certain places within the script, an error is returned when the system validates the script.

Resolving the problem

To avoid this validation error, do not start a comment with two forward slashes. Instead, start the comment with a forward slash and asterisk (/*) and end the comment with an asterisk and forward slash (*/).

Workgroups are not marked as required fields in the Properties widget

Workgroups are not automatically marked as required fields if you are using the system-generated view for the Properties widget.

Symptoms

You add a workgroup to a task in Step Designer. If you use the system-generated view for the Properties widget, the workgroup is included in the view as an optional field.

Resolving the problem

Use one of the following methods to mark a workgroup as required in the Properties widget:

- Create a custom properties layout view that sets the workgroup field to required. Use this view instead of the system-generated view on any page that is used for the task.
- Create a JavaScript to set the required state programmatically by using the following syntax:

  ```
  controller.getPropertyController("Workgroup1").set("required", true);
  ```

  This method marks the workgroup as required in the system-generated view and in any custom views.

Event actions cannot have duplicate labels

An event action that is added to a toolbar or menu is overridden if another event action is added with the same label.

Symptoms

You add an event action to a toolbar or menu in a widget. You then add a second event action to a toolbar or menu in the same widget and give this action the same label as the first action. When open the Wire Events window, only the second action shows in the **Outgoing events** list.

Resolving the problem

To resolve this problem, assign unique labels to the event actions.

Cannot validate case types or deploy a solution after the data type or cardinality of a solution-level property is changed

If you change the data type or cardinality of a solution-level property, you cannot validate the case types that reuse the property and cannot deploy the updated solution.

Symptoms

You changed the data type or cardinality of a solution-level property that is used in various case types, document types, tasks, or steps in the solution. In Case Manager Builder, you try to validate a case type that reuses the property and receive an error such as the following message:

```
Errors occurred when the case type was validated:

t1
Step1: [ ERROR ] Parameter TR_STP1, whose value is (F_CaseFolder.TR_STP1),
Array v. non-array mismatch
Step1: [ ERROR ] Parameter definition value type found float, expected boolean
```

If you try to deploy the updated solution, the deployment fails. When you click **Errors** or **Logs** from the **More Actions** option for your solution on the Manage Solutions page, you see a message in the deployment log that the solution cannot be deployed because there are validation errors. For example, you see the following message:

```
FNRPA0034E The solution cannot be deployed because the validation of the
XPDL document failed with the following Process Engine error message:
TR_t1:Step1:[ ERROR ] Parameter TR_STP1, whose value is (F_CaseFolder.TR_STP1),
Array v. non-array mismatch
TR_t1:Step1:[ ERROR ] Parameter definition value type found float, expected boolean
FNRPA0162E The TR_t1 task workflow does not exist.
FNRPA0093E The previous error was caused by:
[FNRPE2131090101E]Invalid Work Class name: "TR_t1".

FNRPA0162E The TR_t2 task workflow does not exist.
FNRPA0093E The previous error was caused by:
[FNRPE2131090101E]Invalid Work Class name: "TR_t2".
```

Causes

When the data type or cardinality of a property is changed at the solution level, the corresponding instances of the property that are used in case types, document types, tasks, or steps in that solution might not be updated.

Important: Do not change the data type or cardinality of a property if the solution is deployed in a production environment. If you need to change the data type or cardinality of a solution property in a development environment, you must first reset the test environment before you modify and redeploy the solution.

Resolving the problem

In Case Manager Builder, review the validation errors for each case type and update the solution to resolve all the errors. Then, try to redeploy the solution. If the deployment fails again and you see a message in the deployment log that the solution cannot be deployed because there are validation errors, review the errors to determine which part of the solution still must be updated and update the solution accordingly.

Problems occur in Case Manager Client if widgets are configured incorrectly

If certain widgets are not configured correctly for the page on which they are used, the widgets do not work correctly in Case Manager Client.

Symptoms

The widget displays incorrect information or the widget is not functional in Case Manager Client.

Resolving the problem

Ensure that the widget is intended for the page on which it is used and that the widget is configured correctly for the page.

Table 20. Widget

Widget	Restrictions
Attachment	Use this widget only on the following page types: Add Task, Custom Task Details. and Work Detail. Do not use an Attachment widget on the same page as a Form widget that is configured to open by using a form attachment. You can use both widget on the same page if the Form widget is configured to open by using a template.
Case Toolbar	Use this widget only on the following page types: Add Case, Case Details, and Split Case. If you are using the Case Toolbar widget on an Add Case page, the **Display the case title and case type in the Case Toolbar widget** check box is ignored.
Form	Do not use a Form widget that is configured to open by using a form attachment on the same page as an Attachment widget. You can use both widget on the same page if the Form widget is configured to open by using a template.
Original Case	Use this widget only on a Split Case page.
Select Case Documents	Use this widget only on a Split Case page.
Split Case	Use this widget only on a Split Case page.
Work Item Toolbar	Use this widget only on the following page types: Add Task, Custom Task Details, and Work Detail. If you are using the Work Item Toolbar on a Custom Task Details page, do not select the **Display the instructions for the work item** check box. Instead, use the Instructions widget on the Custom Task Details page to display the instructions.

Workflow artifacts are not added to the Process Engine Configuration file when the file is locked

If you insert a workflow into a case type or collection when the Process Engine configuration file is locked, the workflow artifacts are not added to the file.

Symptoms

If the Process Engine configuration file is locked when you are inserting a workflow into a case type, artifacts such as queues, event logs, and rosters are not added to the configuration file.

If the solution is exported and imported to another environment, the workflow might not work correctly.

Resolving the problem

After you insert the workflow, validate the workflow in Process Designer. Fix any errors, or delete the workflow by removing the workflow from the collection. Wait for the Process Engine configuration file to be unlocked, then insert the workflow again.

Unexpected behavior when you use choice lists that have duplicate values with unique display names

You might see unexpected behavior when you use duplicate values in choice lists.

Symptoms

When a solution designer creates a choice list, they can create duplicate values in a single list that have unique display names. For example, an integer choice list might have a value with the display name of First and a value of 1, and another value with the display name of Primary and a value of 1.

The duplicate values are not removed from the choice list. That means that when users select the value, the first instance of the value is selected (in the current example, First). In a multi-value property, if you add Primary, it is converted to First. The Summary view and Case Details view show the value selection as First.

However, if you select the value from a single value property, the behavior changes. You can select Primary from the choice list for the single value property. In this instance, the Summary view displays First, while the Case Details view displays Primary.

You might also encounter issues where the user chooses the second value of two duplicate values, for example, in a check list box editor. The selection might disappear and default to the first instance of the value.

Resolving the problem

If you do not use duplicate values in choice lists, users do not experience the unexpected behavior.

Unexpected behavior when you use different default property values for the same property

Users can experience unpredictable behavior when you configure different default values for separate instances of the same property.

Symptoms

If a view contains two instances of the same property, and each instance is configured with a different default value in the view definition, the results at run time can be unpredictable.

Resolving the problem

If you plan to use multiple occurrences of a property in a view, and plan to define a default value for the property, you must use the same default value for each instance of the property.

Also, if you plan to use a default value for a property, you must specify the default value for each instance of the property in the view. Defining a default value for only one instance of a property that is used multiple times in a view can also cause unpredictable behavior.

If you plan to set the default value in Properties View Designer for a property that will be used in multiple instances, do not configure the default value in Case Manager Builder, in the case type, or by using a starting document type. These other default value settings override the setting you specify in Properties View Designer.

Bi-directional step names do not display in the Step Designer swimlane

Using the Chrome browser in a bi-directional locale can cause display issues in Step Designer.

Symptoms

If you are using Step Designer in a bi-directional locale on a Chrome browser, you might see issues in Step Designer. For example, the name of a step might not display with the step icon after you drag a step to a swimlane.

Resolving the problem

To see the name of the step, select the step to view the full set of properties, including the name, that are associated with the step.

Fields in the Settings pane of the Properties View Designer lose focus in Internet Explorer

If you are working in Internet Explorer, the **Name** field for workflow fields and the **Collection ID** and **Property ID** fields for external properties lose focus each time that you type a character.

This problem, which occurs only if you are using Case Manager Builder in Internet Explorer, forces you to place the cursor in the field after you type each character.

To work around this issue, type the value in a text editor such as Notepad. Then, cut and paste the value into the **Name**, **Collection ID**, or **Property ID** field in the Settings pane of the Properties View Designer.

Focus is lost when some settings in Properties View Designer are changed

When you specify some settings in Properties View Designer by selecting an option from a list, the focus is lost and you must manually restore the focus.

The following Properties View Designer settings are affected by this issue:

- The **Editor** setting in the **Editor Settings** and **Value Editor Settings** areas.
- The **Type** setting in the **Workflow Field** and **External Property** areas.

To restore the focus, click the setting control or press the Tab key until the focus is restored.

The test solution link in Case Manager Builder can redirect to the SiteMinder login page

In a SiteMinder SSO environment, when you click **Test** to preview your solution for the first time, you might be redirected to the SiteMinder login page.

This redirection is inappropriate because you are already logged in to Case Manager Builder. If you try to log in to SiteMinder after you are redirected to the login page, your attempt is unsuccessful. This problem is a known issue in SiteMinder.

To resolve this problem, close the SiteMinder login window and click **Test** again to preview your solution.

Changing the type of a property that is used in in-baskets, in-basket filters, or tasks

Before you change the data type of a property that is used in in-baskets, in-baskets, filters, or tasks, you must remove the property from in-baskets, filters, and tasks.

Before you begin

Important: If the property is already deployed, you cannot change the property type.

About this task

Properties can be defined at the solution level or at the case type level. If you change the data type of a property that is used in any of the following tabs or in a task, you must delete the property references and add them again in the respective places.

- Role In-basket General
- Role In-basket Filters
- Personal In-basket General
- Personal In-basket Filters

Important: In the following procedure, do not click **Save** or **Save and Close** until instructed to do so.

Procedure

To apply property type changes in Role In-basket General and In-basket Filters tabs and case type tasks:

1. Open the solution in Case Manager Builder.
2. Click the **In-baskets** tab
3. Delete the property for each role and personal in-basket.
   a. Select an in-basket.
   b. Click the **In-basket Filters** tab.
   c. Click the **Remove** icon next to the property name that is changing to delete the reference from the list.
   d. Click the **In-basket General** tab.

e. Click the **Remove** icon next to the property name that is changing to delete the reference from the list.

4. Click **OK**.
5. Click **Save**.
6. Change the data type of the property.
   a. Click the **Properties** tab, and then click the name of the property whose data type you want to change.
   b. Select a new type for the property.
   c. In the Confirmation window, click **Yes**.
   d. Click **OK**.
7. Repeat these steps for each case type in the solution:
   a. Click the **Case Types** tab, click the **Case Type** name, and then click **Tasks**.
   b. If the task precondition uses the changed property, edit the precondition.
      1) Click the task name.
      2) Click the **Preconditions** tab.
      3) Select the property, update the operator value, and then click **OK**.
   c. Click the **Edit Steps** icon for the task.
   d. If the **Properties** field for a step uses the changed property, complete the procedure in *Known issue: Changing the property type for a property that is used in a task step* to edit the step properties:http://www.ibm.com/support/docview.wss?uid=swg27020365 .
   e. Repeat steps 7b - 7d for all the tasks that use the property in the precondition or in the step properties parameters.
8. For each task that does not use the property in the step properties, open the task in Step Editor, and then click **Apply**, click **Validate**, and click **Close**.
9. Add the changed property to the role in-basket and filter and personal in-basket and filters as needed.
10. Repeat these steps for each case type in the solution:
    a. Click the **Case Types** tab.
    b. Click the **Case Type** name.
    c. Click **Tasks**, then click the **Edit Steps** icon for the task.
    d. Click **Apply**, click **Validate**, and click **Close**.
11. Click **Validate**, click **Save**, and then click **Close**.

If you change how a task starts from discretionally to manually or automatically, Case Manager Builder does not clear the response from the launch step

For a task that is started discretionally, you can assign a response for the launch step in the Step Editor. Later, if you change the task to start manually or automatically, the response is not cleared from the launch step.

To clear the response from the launch step after you change how the task starts, save and close the solution.

Percent signs (%) and underscores (_) do not work in case property filters

If you include a percent sign (%) or an underscore (_) in a filter value, the filter does not work as expected.

When you build a case, you can enter a string value in the in-basket widget to find work items that contain the specified string in their property values. However, percent signs and underscores create unexpected results if you use them in a filter value.

If you include a percent sign or an underscore in a filter value, no error message is displayed. However, any percent sign or underscore is treated as a wildcard. Rather than returning work items that have a percent sign or an underscore in their property values, the filter returns all work items that have a string with any character in place of the percent sign or underscore.

Adding many properties might cause a script warning message

If you add many properties at a time in Case Manager Builder, you might receive a warning message that a script is taking too long.

Adding many properties can slow system performance or a script might appear to stop running.

If you must add many properties to a solution, especially if you must add many reused properties, try to add the properties in groups of no more than 20. Do not select **Select All** if by doing so, more than 20 properties are selected.

You can also increase the maximum script run time value for your browser.

Inconsistent behavior when adding the same property in multiple in-baskets in the same queue with different object types

If you try to update the object type of a property that is used in multiple in-baskets in the same queue without first saving and closing the solution, the object type might not be set correctly.

For example, you add a property to the All Assigned Work in-basket as a case and then add the same property to the My Work in-basket as a task. After you save and close the solution, the property is still set as a task in both in-baskets.

To work around this issue, save and close the solution before you change the object type of a property that is used in multiple in-baskets.

Tasks cannot be assigned to new sets before you save and close the solution

If you create a set in Case Manager Builder and then try to assign an existing task to that set, the task is not successfully assigned to the set.

To work around this problem, save and close the solution after you create a set and before you assign tasks to that set.

Unexpected results when you use a number spinner editor with a property of type float

In Case Manager Builder, you configure a float property to use a number spinner editor and you select the **Round automatically** option. In Case Manager Client, the value of that property is unpredictable if the user clicks the arrows in the number spinner multiple times.

To avoid problems with float properties that use a number spinner, use the following guidelines to configure the property in the Properties View Designer:

- Specify an initial value for the property, either in the model layer or by setting the default value in Case Manager Builder.
- Select the **Round automatically** option.
- Specify the number of decimal places.
- Specify reasonable values, such as 1 or 0.25, for the **Small increment** and **Large increment** fields. (Setting these fields to values such as 0.333 can cause problems.)

Preventing users from having to select a folder when they add documents

You can configure a case type setting in Case Manager Builder that allows users to add documents from non-case management repositories. However, with this setting, users might be required to select a folder when they add a document.

About this task

To prevent users from having to select a folder when they add documents, you can change a default setting in your IBM Case Manager desktop:

Procedure

1. As an administrator in IBM Content Navigator, navigate to **Desktops** > **Case Manager** .
2. Click the **General** tab, then expand the **Desktop Configuration** settings.
3. Under **Additional Settings**, clear the setting **Require users to save new documents and folders in a folder**.
4. Save your changes.

Earlier minor versions of Internet Explorer 10 or 11 can cause issues with Case Manager applications

If your browser is an older, minor version of Internet Explorer 10 or 11, you might experience unexpected behavior in Case Manager Builder and Case Manager Client.

For example, you might find that in Case Manager Builder, you cannot add a filter to an in-basket. In Case Manager Client, you might find that some static pages do not open as expected.

To resolve these problems, use another supported browser to access your case management applications. If you want to use Internet Explorer 10 or 11, update the browser to the latest available version.

Certain property templates cannot be used in IBM Case Manager

Certain property templates cannot be used in IBM Case Manager properties.

IBM Case Manager does not support the following types of property templates:

- Multi-value property templates of type unique and unordered
- Property templates with hierarchical choice lists

Case and attachment documents with non-English-language titles are added to email with incorrect titles

When you use the Case Information widget or the Attachment widget, case documents and attachment documents that have a non-English-language title are added to email with the incorrect title.

Titles for English documents are correct in the email. For example, a graphic that has an English title is correctly labeled `MyGraphic.jpg` when it is added to email. A graphic with a non-English-language title is incorrectly labeled `wcEmail.jpg` when it is added to email.

Cannot access Process Designer from Case Manager Builder with Google Chrome

Because Chrome no longer supports Java applets, you cannot access Process Designer from Case Manager Builder when you are using Chrome.

To use Process Designer, open Case Manager Builder in either Mozilla Firefox or Microsoft Internet Explorer.

Queue changes might not take effect after a solution is deployed

When you edit a solution workflow collection by using the Process Configuration console that is launched from Process Designer, changes to queue security and component queue properties might not take effect after the solution is deployed.

Symptoms

For example, if you remove a user from queue security, the change will not take effect. Conversely, if you add a user to queue security, the change does take effect.

Resolving the problem

To change queue security and component queue properties, use Administration Console for Content Platform Engine.

Troubleshooting Case Manager Client

Troubleshoot typical errors that might surface in the Case Manager Client.

Related troubleshooting information

"A case cannot be created if the initiating document title contains a vertical bar (|)" on page 232

"Tasks cannot communicate with a business process" on page 233

"Reducing the time needed for advanced searches" on page 235

"Changing the screen display resolution for Case Manager Client and Case Manager Builder" on page 212

"A search returns too many results" on page 236

"Prompt to stop the script is displayed when searching for cases" on page 237

"Sending a link to a case in an email opens an empty tab in the Firefox browser" on page 237

"Incrementing float values in number spinner property fields" on page 237

"Filtering the in-basket with an (is-like) filter returns only exact matches" on page 239

"Cannot add values to multi value properties" on page 239

"Case History shows extra task states for tasks that are configured with the Automatically completed when a case completes setting" on page 240

"Document Modified events do not display in the histogram" on page 240

"Box actions are not displayed in the Documents view for existing solutions" on page 247

"Case packaging action is not displayed on Case Details or Cases page for existing solutions" on page 248

"Text in case package PDF file is not displayed correctly" on page 248

"Unicode names are incorrect in case package for documents with non-English characters in the file name" on page 249

"The file does not open when you click a link to a .zip file in a case package" on page 250

"Restarting an IBM Content Manager task that fails to start" on page 250

"Box Collaboration action fails in a distributed environment when the date/time is not synchronized" on page 252

Related concepts

"Errors in Case Manager Client property settings" on page 239

"Forms created with IBM FileNet eForms for P8 or IBM Forms do not work with IBM Case Manager after you import them into Content Engine" on page 240

"Reserved words cannot be used in solution names" on page 240

"Cannot open a view that contains a datetime property with an invalid mask or pattern" on page 241

"The time mask pattern K does not work in Case Manager Client" on page 241

"Some property values are empty for cases that are returned by a search that uses the icm.util.SearchPayload class" on page 241

"Form templates used with the Case Form widget cannot be stored in IBM Content Manager" on page 242

A case cannot be created if the initiating document title contains a vertical bar (|)

Some cases are created automatically when you add a specific type of document. However, if the title of an initiating document contains a vertical bar (|), Case Manager Client cannot create the case.

Symptoms

You add a document of the specified type to a case or work item and include a vertical bar in the title. Case Manager Client attempts to create a new case, but the case state remains in the initializing state.

Resolving the problem

Delete the document with the vertical bar in the title from the attachment. Add the document to the attachment again without including a vertical bar in the title.

Tasks cannot communicate with a business process

You might encounter problems in which a task fails to communicate with a Business Process Manager Advanced business process that it starts.

Symptoms

You might experience the following problems if a task and business process cannot communicate:

- The task is started, but the web service for the business process is not invoked.
- The task does not receive a response from the web service, so the case properties are not updated as expected.

On the Business Process Manager Advanced, you can use the failed event manager to find failed events for your web service.

Causes

These problems might occur in the following situations:

- The response address that identifies where the web service is to send the response is not correct.
- The component manager for the isolated region where the task is deployed is not started. The component manager must be started so that it can deliver events from IBM Case Manager to the web service.
- The web service was not deployed or was not started. The web service must be available and running to receive events from IBM Case Manager.
- The authentication credentials are not set correctly to permit communication between the task and the web service.
- If the web service moved to a different server, the XPDL document that contains the task might contain the wrong endpoints for the web service. The XPDL document, which is created by Integration Designer, uses these endpoints to locate the web service that is associated with a task.

Diagnosing the problem

To enable tracing in the IBM Case Manager environment, make the following changes in the `P8BPMWSBroker.properties` file.

- Set `filenet.ws.listener.tracefile` to a valid path and file name.
- Set `filenet.ws.listener.tracing` to `true`.
- Set `filenet.ws.request.tracefile` to a valid path and file name.
- Set `filenet.ws.request.tracing` to `true`.

Tip: The `P8BPMWSBroker.properties` file is in the following Workplace XT installation folder: *`install_location`*`/FileNet/WebClient/WorkplaceXT/WEB-INF`

If you cannot identify the problem, enable tracing in both the IBM Case Manager environment and the Business Process Manager Advanced environment.

To enable tracing in the Business Process Manager Advanced environment:

1. Open the administrative console.
2. Click **Troubleshooting** and then click **Log and Trace**.
3. Click the server on which your web service is located.
4. Click **Change log detail levels** and then click the **Run time** tab.
5. Expand the tree and select **SCA** and **com.ibm.ws.webservices** to enable tracing.

In addition, check the Business Process Manager Advanced administrative console for any failed callbacks:

1. Open the administrative console.
2. Click **Integration Applications**.
3. Click **Failed Event Manager**.

Resolving the problem

To resolve this problem, perform the action that corresponds to the problem that you identified:

The response address is not correct

Ensure that the Listener URL endpoint that is configured in Component Manager is valid. Ensure that the Business Process Manager Advanced can reach the Listener URL endpoint.

Component manager is not started

To start the component manager:

1. In Process Task Manager, expand the **Component Managers** node and select the component manager for the isolated region where the deployed task is running.
2. Click **Start** on the toolbar.

The web service is not deployed or the web service endpoints are not correct

Deploy the web service module into the target Business Process Manager Advanced runtime environment. For instructions, see the Business Process Manager Advanced documentation.

If the web service moved to a different server, configure the web service endpoint URL information for HTTP bindings. For instructions, see the Integration Designer documentation for the feature pack.

Then, use FileNet Deployment Manager to update the `PE Partnerlink` element in the solution definition for the target environment and redeploy the solution.

The web service is not started

On the Business Process Manager Advanced, use the administrative console to ensure that the web service is running.

Authentication credentials are not correct

When you create the web service module, you can specify that user name and password credentials are to be supplied when an IBM Case Manager task invokes a web service module on Business Process Manager Advanced. Optionally, you can use a secure socket (SSL) connection to provide an additional level of security for the request from IBM Case Manager to Business Process Manager Advanced.

To ensure that security is correctly configured from IBM Case Manager, use the Component Managers function in Process Task Manager to verify authentication credentials.

After you correct the problem, you must resubmit the task request. To do so, use Process Administrator to locate the request in the Conductor queue and complete the Review step.

Reducing the time needed for advanced searches

When you search over large numbers of items, you might need to create an index on any custom user properties that are used in a WHERE condition. If you do not create an index, the search can take a long time because it performs a table scan.

Symptoms

A search that contains a WHERE condition on a user property takes several minutes to complete.

Resolving the problem

To optimize performance of searches, ensure that you have an index that corresponds to each of the most important searches that are run during working hours. However, too many indexes can degrade performance. Therefore, if you have many different ORDER BY conditions or search conditions, create only those indexes that will improve performance for most searches.

Important: If a database contains a large amount of data, performance can be degraded even if you use indexes for searches. For example, searching a database that contains more than 250 KB of data will take a long time even if you use an index.

Tip: In addition to using indexes, you can improve search performance by including conditions to limit the number of rows that are returned by the search.

Typically, the type of searches each system uses varies. You must analyze your common search queries to determine which of the indexes shown in the following examples are correct for your searches.

Example 1

Assume that you have the following search:

```
SELECT * FROM ECMPerfCase1 WHERE (CmAcmCaseState = 2 AND
  cmis:createdBy = 'user_2')
ORDER BY CmAcmCaseIdentifier ASC.
```

If this search involves more than one user and more than 20,000 cases, ask the database administrator to create an index as shown in the following examples.

Tip: The database administrator must use the actual column names for the indexed elements. To obtain the full column names, including the u<xy>_ prefix, issue the **describe table** command for the container table from any SQL tool.

- If the search returns only a few results, use the following index:

  ```
  create index I_CREATOR_STATE on Container (creator,
  u<xy>_CmAcmCaseState)
  ```

- If the search returns a large number of matches, sorting by the ORDER BY CmAcmCaseIdentifier element might take too much time. In this situation, use the following index:

  ```
  create index I_CREATOR_STATE_ID on Container (creator,
  u<xy>_CmAcmCaseState, u<xy>_CmAcmCaseIdentifier)
  ```

Example 2

Assume that you have the following search:

```
SELECT * FROM <case type> WHERE (CmAcmCaseState = 2 AND
   cmis:lastModifiedBy = <user_name>)
ORDER BY CmAcmCaseIdentifier ASC
```

Ask the database administrator to create the following composite index:

```
create index I_ModifyUser_STATE_ID on Container (modify_user,
u<xy>_CmAcmCaseState, u<xy>_CmAcmCaseIdentifier)
```

Example 3

Assume that you have the following search:

```
SELECT * FROM ECMPerfCase1 WHERE (CmAcmCaseState = 2 AND
   cmis:createdBy = 'user_2'
AND CCDM_customername= 'value1')
ORDER BY CmAcmCaseIdentifier ASC
```

Ask the database administrator to create the following composite index if:

- An index such as the `I_CREATOR_STATE_ID` index shown in Example 2 is not used in the query plan for this search.
- An index such as the `I_CREATOR_STATE_ID` index is used, but the index scans are still taking a long time.

```
create index I_CNAME on container (u<xy>_CCDM_customername, creator,
u<xy>_CmAcmCaseState, u<xy>_CmAcmCaseIdentifier)
```

Changing the screen display resolution for Case Manager Client and Case Manager Builder

The default screen size for Case Manager Client and Case Manager Builder can be too large for small computer monitors with low resolution (for example, 768x1080).

Symptoms

A scroll bar is displayed at the bottom of the screen.

Causes

The default screen resolution assumes larger computer monitors with large screen resolution settings. Smaller computer monitors with low resolution require a horizontal scroll bar to view the entire application.

Resolving the problem

Press Ctrl+minus sign key (-) to fit the entire application on a low resolution screen without the horizontal scroll bar.

Note: This workaround does not change the configured screen resolution; it changes the size of the application within the browser.

A search returns too many results

If you do not specify the criteria correctly in the Advanced Search dialog box, an unexpectedly large number of results can be returned.

Symptoms

In the Advanced Search dialog box, you select **Any** from the **Match Criteria** list. You do not select a value from the **Case State** list. When you run the search, the number of results that are returned exceeds what you expected.

Causes

If you do not specify a case state in the search criteria, IBM Case Manager automatically sets the case state to greater than or equal to `Working` and adds it to the query. Because IBM Content Navigator does not handle a query that contains both `AND` operators and `OR` operators, the resulting query uses an `OR` operator as shown in the following example:

```
"Case State >= Working" OR Prop1 = "a" OR Prop2 = "b"
```

This statement returns all cases that are in the working, failed, or complete state.

Resolving the problem

To resolve the problem, the solution designer can create a custom search widget that handles queries that contain both `AND` operators and `OR` operators.

Prompt to stop the script is displayed when searching for cases

If a search for cases takes a long time, your web browser displays a dialog box that asks if you want to stop the script.

Symptoms

If you initiate a search for cases from the Cases page, your web browser displays a dialog box if the search takes take a long time to run. The dialog box prompts you to decide whether to stop the script.

Resolving the problem

Click **No** to continue the script and complete the search.

You can avoid this problem by increasing the script timeout value in your web browser.

Sending a link to a case in an email opens an empty tab in the Firefox browser

If you use Mozilla Firefox as your browser, a blank tab might be left open if you select the **Send Link to Case** in the Case List widget menu or **Send Link to Case by Email** in the Case Toolbar widget.

Symptoms

If you use Firefox and you did not configure a default email client, Firefox prompts you to select an email client the first time that you select one of the following actions:

- **Send Link to Case** in the Case List widget menu
- **Send Link to Case by Email** in the Case Toolbar widget.

The Firefox dialog box opens in a new tab so that your work in Case Manager Client is not affected. If you select a web email client, the login page for that email client opens in this tab. If you select a desktop email client, the email client opens in your desktop. However, the blank tab remains open in the browser.

Resolving the problem

Close the blank tab in the browser. The empty tab does not prevent you from sending the link.

Incrementing float values in number spinner property fields

Case Manager Client users may encounter issues with number spinner controls when the value in the field is a float type.

Symptoms

Some solutions are designed so that certain number values can be changed within their property field using a number spinner, which can increment the value up or down by a specified amount. However, when the number is a float type, an incremental increase or decrease can have undesirable results. Number spinner property fields can run into issues in several rare situations, such as when:

- No default value is specified for the property in Case Manager Builder. When a Case Manager Client user increments a number spinner property field up or down with no starting value, then the minimum or maximum value for that float value will be displayed.
- The value specified for either the large or small increment is a decimal with a specified number of decimal places. Due to certain javascript storage factors, incrementing by decimals can result in numbers that are slightly more or less than the expected value. For example, if the value for a property is meant to contain a US Dollar amount, then the number of significant decimal places is 2, and the number spinner might reasonably be set to increment by `0.01`. However, a user incrementing `1.05` up might get a result of `1.060000000997`, instead of `1.06` as expected.
- The value specified for either the large or small increment is not accurate due to rounding errors. For example, if the number spinner is set to increment by `1/3`, and the number of decimal places is 2, the value for the increment will be inaccurate since `1/3` cannot be expressed by a decimal with two digits (either `0.33` or `0.34` might be used, neither of which is precisely accurate). Consequently, incrementing the number spinner will begin to cause number errors with each increment. In the example, incrementing up by `1/3` from a starting value of `0.00`, using increments of `0.33`, will first yield results of `0.33` and then `0.66` after two increments. However, the second increment value of `0.66` is not accurate, as the correct rounded value for `2/3` is `0.67`. While this might be temporarily corrected by using a more precise increment (for example, `0.333` instead of `0.33`, this will only delay the first inaccurate number until more increments have been applied.

Resolving the problem

There are a number of solutions to these issues that can be applied depending on the situation.

- You should always define a default value for the property. This will prevent Case Manager Client from using the maximum or minimum value for a float number as the result of a first increment.
- When a property is to be incremented by a specified decimal value, you should specify the number of decimal places when designing the property in Case Manager Builder. You should also specify that the number should be automatically rounded. When dealing with increments with repeating decimals, choose a meaningful number of decimal places and specify the increment as accurately as possible to avoid rounding errors as best as possible for your solutions needs.

To modify the attributes of a property's number spinner, such as the large and small increments, number of decimal places, and whether the value should be automatically rounded:

1. Open the solution in Case Manager Builder and click on the property with the number spinner that you want to modify.
2. Click on the **Case Types** tab, and click on the desired case type.
3. Click **Views** in the left navigation.
4. Click the **Properties Layout** tab, and click the desired view.

5. In the Properties area, click on the property that contains the number spinner field that you want to modify.
6. Click on the number spinner field. The settings for the number spinner can be found in the Control Settings area.

Errors in Case Manager Client property settings

In Case Manager Client, you can recover from some errors in property fields.

Users might encounter error conditions on number spinner properties, date, or datetime field properties.

Use the following tips to recover from the errors:

- If you encounter an error in a number spinner field, click the arrows to the correct value, or edit the numbers directly.
- If you encounter an error with a date or datetime field, you can edit the value with the calendar tool or by using the keyboard. To use the keyboard, tab out of the field and then use the Shift + Tab back into the field. You can then use the arrow key to position the cursor at the point where you want to edit.

Filtering the in-basket with an (is-like) filter returns only exact matches

When you use an (is-like) filter for your in-basket, you see only exact matches returned.

Symptoms

If you enter a value for the (is like) filter for an in-basket, you expect to see filtered returns that are similar to the value that you enter. However, only exact matches are returned.

Resolving the problem

When you enter a value for the (is like) filter, add the wildcard character % to the value. This wildcard expands the scope of the filter.

Cannot add values to multi value properties

It is not possible to add values to multi value properties because the **OK** button on the data entry window is not visible.

Symptoms

You attempt to add a value to a multi value property, but the bottom of the data entry window that contains the **OK** button is hidden.

Causes

Because the property view was designed with a multi value property that is displayed at the bottom of the page, the **OK** button on the data entry window is hidden.

Resolving the problem

Try one of these methods to change the position of the data entry window:

- Resize the browser window in the vertical direction.
- If the properties widget or browser window contains a vertical scroll bar, scroll down.

Then try to add a value to the multi value property again.

Case History shows extra task states for tasks that are configured with the Automatically completed when a case completes setting

Some Automatically completed tasks show extra states in the Case History.

Symptoms

Some tasks can be configured to complete when the case completes. To move these tasks to the Complete state, IBM Case Manager must first move the task from Working to Failed/Cancelled to Working to Complete state.

Resolving the problem

These states display in the Case History, giving the impression that the tasks moved through extra unnecessary states. However, this transition of states is an artifact of the process of completing this type of task, and the Complete state at the end of the process is correct.

Document Modified events do not display in the histogram

Changes to a document in a case do not display in the histogram of the Case History Visualizer.

Symptoms

When you modify the properties of a case document, the event does not display in the histogram area of the Case History Visualizer.

Resolving the problem

The histogram is intended to display a summary of case activity. Because document changes are not necessarily tied to an individual case, these changes are not included in the case histogram. You can use the timeline view to track Document Modified events.

Forms created with IBM FileNet eForms for P8 or IBM Forms do not work with IBM Case Manager after you import them into Content Engine

To use a form that was created with IBM FileNet eForms for P8 or IBM Forms with IBM Case Manager, you must select the `ITXFormTemplate` class or one of its subclasses as the document class when you import the form into Content Engine.

In addition, to import a form that was created with IBM Forms or to attach that form to a case, the form must have a `.xfdd` file extension.

Reserved words cannot be used in solution names

IBM FileNet Process Engine reserved words cannot be used in IBM Case Manager solution names.

For more information, see the IBM FileNet P8 Version 5.2.1 Knowledge Center for a list of reserved words.

Cannot open a view that contains a datetime property with an invalid mask or pattern

If you define an invalid mask or pattern for a datetime property in Properties View Designer and then you save and close the view, you cannot reopen that view in Properties View Designer. If you deploy a solution and try to open a work item in Case Manager Client, the view does not load.

For example, `hh - mm - ss A` is an invalid time pattern for a single value datetime property. The correct syntax is `hh - mm - ss a` (where the `a` is lowercase).

After you set a mask or pattern for a datetime property, you can test it by assigning a default date for the property in Properties View Designer. If the mask or pattern does not seem to be applied correctly for the default value, then it is likely that the mask or pattern is not valid in Properties View Designer. For example, if you specify `A` instead of `a`, then AM or PM does not display as part of the default value. You can also deploy the solution and verify that the datetime properties are displayed correctly in Case Manager Client.

Tip: For more information about datetime formats, see http://dojotoolkit.org/reference-guide/1.9/dojo/date/locale/format.html#id3.

The time mask pattern K does not work in Case Manager Client

In Properties View Designer, you can specify the pattern of date and time fields by using standard date and time mask patterns. Choosing the K pattern for the time mask, however, can lead to validation errors.

If you specify the K pattern for a property, Case Manager Client users can see an error on the field like the following one: `"The value entered is not valid."`

To resolve this issue, specify a different time mask pattern for your date and time fields in Properties View Designer.

Some property values are empty for cases that are returned by a search that uses the icm.util.SearchPayload class

If you write a custom search that uses the `icm.util.SearchPayload` class and your solution contains multiple case types, property values in the returned cases might be empty.

To ensure that the correct property values are returned, set the search case type for the `icm.util.SearchPayload` class. To set the search case type, add the following line to your custom code:

```
payload.searchTemplate.setClasses([new ecm.model.SearchClass(
    caseType_Identifier, caseType_Identifier, "folder", true)]);
```

The following example shows how this line is used in custom code.

```
var solution = this.solution; // solution from the widget.
var params = {};
params.ObjectStore = solution.getTargetOS().id;

var criterion = new ecm.model.SearchCriterion({"id":
    "ICM_strField", "name": "ICM_strField", "selectedOperator":
    "EQUAL", "dataType": "xs:string", "defaultValue" : "1234",
    "value": "1234", "values": ["1234"]});
```

```
params.criterions = [criterion];

// params.ceQuery = "SELECT t.[FolderName], t.[LastModifier],
    t.[DateLastModified], t.[CmAcmCaseTypeFolder],
    t.[CmAcmCaseState], t.[CmAcmCaseIdentifier], t.[DateCreated],
    t.[Creator], t.[Id], t.[ContainerType], t.[LockToken],
    t.[LockTimeout],  t.[ClassDescription], t.[DateLastModified],
    t.[FolderName] FROM [CmAcmCaseFolder] t WHERE
        ((((t.[CmAcmCaseIdentifier] LIKE '%%' or
        t.[CmAcmParentSolution] =
        Object({201323A3-271B-48CC-9C0D-7D0B20B1822C})) and
        t.[CmAcmCaseState] > 1) )) ORDER BY
        t.[CmAcmCaseIdentifier]";

params.CaseType = "ICM_CaseType1";
params.solution = solution;

var searchPayload = new icm.util.SearchPayload();
searchPayload.setModel(params);

var self=this;
searchPayload.getSearchPayload(dojo.hitch(self, function(payload) {
    payload.searchTemplate.setClasses([new ecm.model.SearchClass("ICM_CaseType1",
    "ICM_CaseType1", "folder", true)]);
    self.onBroadcastEvent("icm.SearchCases", payload);
}));
```

Form templates used with the Case Form widget cannot be stored in IBM Content Manager

If you configure the Case Form widget to use a form template as an interface to collect data, you must store the form template in an IBM FileNet Content Manager object store. You cannot store the form template in a IBM Content Manager repository.

You cannot use the number grouping characters in integer or float values in IBM Case Manager

You cannot use the number grouping characters for your locale as separators in IBM Case Manager numeric fields.

Due to a known issue with IBM Content Navigator, number fields in the following IBM Case Manager components cannot accept characters to separate digits. For example, the components cannot accept commas or periods to separate thousand digits.

- Search widget
- Case list widget
- In-basket widget
- Document properties

The Properties widget and the Summary tab of the Case Information widget still accept number separators.

For more information about the IBM Content Navigator known issue, see: Content Navigator known issue: You cannot use the number grouping characters for your locale in IBM Content Navigator numeric fields.

You cannot delete a table row by clicking the Delete icon in the Form widget if you are using an IBM FileNet P8 eForms template

If you are using an IBM FileNet P8 eForms template and you try to delete a table row by clicking the **Delete** icon in the Form widget, the row appears to be deleted. However, when you reopen the Case Details page or Work Details page, the row is still displayed in the Form widget.

Instead of deleting the row, delete the value from each cell of the row.

Some property containers are not displayed in Internet Explorer 9

If you run Case Manager Client in Internet Explorer 9, some containers might not be displayed if the property view contains a scroll bar for a horizontal list of radio buttons.

To work around this problem, in Case Manager Builder, increase the value of the Field width setting for the associated choice list property. Ensure that you specify a large enough width so that no scroll bar is needed.

The Browse button is disabled after you cancel from the Run Content Navigator File Tracker window

When you add a document to a case, if you click **Cancel** from the Run Content Navigator File Tracker window, you can no longer browse for a document to add.

When file tracking is enabled in IBM Content Navigator, you are prompted to run the file tracker feature when you browse for a document. If you close the window by clicking **Cancel**, you return to the Add Document window. However, the **Browse** button is disabled, preventing you from browsing to the document that you want to add.

To resolve this problem, close the Add Document window, clear the browser cache, then close and restart the browser. When you return to the case, you should be able to use the **Browse** button on the Add Document window. When you see the Run Content Navigator File Tracker window, click **Run**, and in the next window, click **Allow**.

Tip: In both of the File Tracker windows, you can choose not to see the windows again in subsequent document add operations.

Unexpected viewer behavior in Case Manager Client when you open documents for which the MIME types are not configured

When the viewer for Case Manager Client is not configured for the relevant document MIME type, the viewer prevents you from viewing a document a second time.

You can open a document for viewing on a page that contains the Viewer widget, such as the Work Details page. You can then download the document, view the document in the native application, or cancel the operation. However, because the document tab persists in the viewer window, you cannot view the document again.

To resolve this problem, close the document tab. You can then view the document again.

To prevent this behavior, configure the Viewer widget to always open documents in a new window.

Some search documents do not behave as expected when added to specific widgets

Some search documents that are created in IBM Content Navigator do not behave as expected when they are added to specific widgets.

Issues occur with a saved search in IBM Content Navigator that prevent you from adding these search documents to the Case Document widget.

You can add these search documents to the Work Item Attachment widget, and the documents can be opened. However, the documents do not perform a search or display search results.

Changes in task property events are not shown in the Timeline Visualizer widget

Changes in task property events are not captured in the case history unless you correctly configure the **TimeToLive** JVM parameter on your Content Platform Engine server.

To ensure that the Content Platform Engine server captures changes in task property events, set the **TimeToLive** JVM parameter on the server to 1 minute as follows:

```
-DFileNet.CMC.TimeToLive=60000
```

This setting works with the built-in settings of 5 minutes for the case history cache on classes and the 2-minute sleep time for case history event capture to ensure that the server captures the changes in task property events.

Tip: After you configure task property auditing, allow some time for the case history to reflect the configuration and begin capturing the event changes. The changes are then visible in the Timeline Visualizer widget.

CmAcmCaseState never automatically resets from Completed to Working even when new task instances are launched for a completed case

When the caseState (CmAcmCaseState) property is set to Completed (3), IBM Case Manager does not change the caseState property value back to Working (2) if a disabled task is enabled or if the re-enabled task is then launched. Once a case is marked as Completed, IBM Case Manager does not change the caseState.

If you want to reset the caseState (`CmAcmCaseState`) property in this scenario or in a similar scenario, you can do so in one of several ways:

- Manually in Administration Console for Content Platform Engine
- In their Workflow map design
- By using custom code

Different browsers can display workflow group fields differently in Case Manager Client

Depending on the browser that you use, fields that include workflow groups in a system-generated view can display in different orders in Case Manager Client.

Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome have different sorting algorithms. Different algorithms can cause differences in the order that is used to display fields that include workflow groups. For example, in one browser, workflow groups might display at the top of the view while in another browser, workflow groups might display at the bottom of the view.

If you want to avoid this issue, always use the same browser to access Case Manager Client or use a user-created property view.

Some container types in the Properties View Designer are incompatible with certain locales

Using some container types in Properties View Designer in some locales can cause the view to become corrupted.

In Properties View Designer, if you specify a tabbed container or a titled container in one of a number of affected locales, you might find that the view is corrupted the next time that you open it. The properties that you included in the view are no longer visible.

The following locales are affected:

- Arabic
- German
- Spanish
- Finnish
- Hungarian
- Norwegian
- Polish
- Portuguese
- Portuguese-Brazilian
- Romanian
- Slovak
- Thai

If you are creating solutions in one of these locales, do not use tabbed or title containers in Properties View Designer.

Cannot cancel the check-out of documents in Case Manager Client that were added from an Alfresco CMIS repository

You can add documents from an Alfresco CMIS repository as case documents or as attachments.

However, if the case folder contains external documents, the Cancel check out action is disabled for the documents from the Alfresco CMIS repository after you perform a Checkout action. Thus, you cannot cancel the check-out of the documents in Case Manager Client.

To work around this issue, browse to the documents in the Alfresco CMIS repository and cancel the check-out.

Inconsistent user interface behavior with bidirectional locales in IBM Case Manager

When you run IBM Case Manager on a browser that uses a bidirectional locale, some aspects of the user interface do not display consistently.

IBM Case Manager supports basic right-to-left and left-to-right language content, but it does not support more complicated bidirectional text.

IBM Case Manager does not support non-Gregorian calendar controls or date time formatting.

Because Case Manager Client is a plug-in of IBM Content Navigator, any bidirectional text, calendar, or date time issues for IBM Content Navigator can also apply for IBM Case Manager.

When IBM Forms is used in a cluster for IBM Case Manager, a failover on the IBM Case Manager server can cause unexpected behavior

When IBM Case Manager with IBM Forms is configured to fail over, you might find that property updates in the client are not saved in the expected way.

This scenario occurs when IBM Case Manager uses IBM Forms, and you are updating properties in a form. Before you save the property values, the system experiences a failover. When you try to edit and save property values, you might see an error message like the following message: `We have experienced a minor service disruption that may have caused some loss of data. Please review your form to make sure that all of the information is intact.`

Click **OK** in the window one or more times to dismiss the message. When you close and reopen the work item, you might notice that different values are displayed now than were displayed after you dismissed the error message. Verify and make the updates again, if needed, then click **Save** twice. Close and reopen the work item to see the values that were updated and saved.

This known issue from IBM Forms can be resolved by applying an IBM Forms fix pack that contains a fix for this issue.

Documents from external repositories cannot be removed or unfiled from a case folder if Content Platform Engine uses a database other than DB2

Normally, you can remove or unfile a document from a case folder by using Case Manager Client. However, if the document is from a non-case management (external) repository and if Content Platform Engine uses a database other than DB2, you cannot remove or unfile the document. If you attempt to remove or unfile the document, you encounter an error.

Favorites and sync features are not supported for IBM Case Manager documents from repositories other than IBM FileNet P8

You cannot use the favorites and sync features on case documents that are stored in external repositories such as IBM Content Manager and CMIS repositories.

IBM Case Manager reuses the favorites and sync features from IBM Content Navigator. These features are not supported, however, for documents that are in external repositories. An *external repository* is a repository other than FileNet P8 that was originally configured for IBM Case Manager.

For example, for an IBM Content Manager repository, the IBM Content Navigator Administration Console does not show the Sync enabling feature for configuration. The feature is only available for enabling on FileNet P8 repositories. Normally, the feature is enabled on the target object store where the solution is deployed.

Box actions are not displayed in the Documents view for existing solutions

The Box actions are not displayed in the Documents view for existing solutions.

Symptoms

The Box collaboration actions are not displayed:

- The **Add Box Collaboration Folder** action is not displayed in the menu of the Documents view.
- The **Manage Collaborators** and **Assign Box Task** actions are not displayed for the Box collaboration folder.
- The **Box Copy** action is not displayed for case documents in Content Platform Engine or documents in the Box collaboration folder.

The **Box Share** and **Delete Box Share** menu actions are not displayed for a case document or attachment from Content Platform Engine or IBM Content Manager.

Resolving the problem

The Box collaboration actions are displayed by default in the Documents view for solutions that are created after Box collaboration is enabled. But for solutions that were created before Box collaboration was enabled, you must manually add these actions by editing the solution in Case Manager Builder. For instructions, see Adding Box collaboration actions for existing solutions.

The **Box Share** and **Delete Box Share** menu actions are displayed by default in the Documents view for solutions that are created in IBM Case Manager version 5.2.1 Fix Pack 3 or later. For solutions that were created before Fix Pack 3, the actions

must be manually added by editing the solution in Case Manager Builder. For instructions, see Adding Box Share menu actions for existing solutions.

Case packaging action is not displayed on Case Details or Cases page for existing solutions

The case packaging action is not displayed on the Case Details or Cases page for existing solutions.

Symptoms

For solutions that were created before version 5.2.1 Fix Pack 4, the **Create Package** button is not displayed in the Case Toolbar widget on the Case Details page and the **Create Package** menu action is not displayed in the Case List widget on the Cases page in Case Manager Client.

Resolving the problem

For solutions that are created in version 5.2.1 Fix Pack 4 or later, the case packaging action is displayed by default on the Case Details and Cases pages. For solutions that were created before Fix Pack 4, the case packaging action must be manually added by editing the solution in Case Manager Builder.

To add the case packaging action to a solution that was created prior to version 5.2.1 Fix Pack 4:

1. Open the solution in Case Manager Builder.
2. Add the **Create Package** button to the Case Toolbar widget on the Case Details page.
   a. On the **Pages** tab, open the Case Details page.
   b. In Page Designer, click the **Edit Settings** icon for the Case Toolbar widget.
   c. On the **Toolbar** tab, select the **Editing a case** toolbar.
   d. Click the **Add Button** icon and select the **Create Package** action.
3. Add the **Create Package** menu action to the Case List widget on the Cases page.
   a. On the **Pages** tab, open the Cases page.
   b. In Page Designer, click the **Edit Settings** icon for the Case List widget.
   c. On the **Menu** tab, click the **Add Menu Item** icon and select the **Create Package** action.
4. Save and redeploy the solution.

Text in case package PDF file is not displayed correctly

In the PDF file that is included in a case package, some text is not displayed correctly.

Symptoms

For a case package that is generated for a locale other than English, or the case data is in a language other than English, some or all of the text is not displayed in the PDF file. Instead, a number sign (#) is displayed in place of each character.

Causes

The required font file for your locale is not found. Either the font directory is not specified correctly in the configuration file, or the required font file is not installed on the computer.

Resolving the problem

1. Verify that the font directory is specified correctly in the case package configuration file. In most cases, the font directory is automatically detected. But if the font directory is not in the default location, you might need to manually specify the path to the font directory:
   a. Open the *network_shared_directory*/AddOns/casePackage/userconfig.xml file in your development and production environments.
   b. In the <fonts> element, verify that the value of the <directory> element is correct. For example, the default font directory on Windows is C:\Windows\Fonts. If the value is not correct, update the file.
2. Ensure that the required font for your locale is installed on the computer:
   a. Open the *network_shared_directory*/AddOns/casePackage/casepackage_font.properties file in your development and production environments to determine which font is required to generate PDF files for your locale.
   b. Install the specified font on your computer, or update the file to specify a different font that is already installed on your computer.

Important: If you modify the userconfig.xml or casepackage_font.properties file, back up the modified file before you install a patch or run the Register the IBM Case Manager Administration Client Plug-in configuration tool task. When you install a patch or run the Register the IBM Case Manager Administration Client Plug-in configuration tool task, the modifications to the files are overridden.

Unicode names are incorrect in case package for documents with non-English characters in the file name

When a case document has non-English characters in the file name, the case package contains the correct file name. However, the characters are scrambled in the tooltip and the security warning that are associated with the file.

Symptoms

You add a case document with non-English Unicode characters in the file name to a case package. The document is added to the case package as a .zip file and the package PDF file contains a link to this .zip file. You then use a third-party utility to open the .zip package or extract the document from the .zip package. The file name of the document is incorrect because the non-English Unicode characters in the name are scrambled.

Resolving the problem

Take one of the following actions to resolve this problem:

- Continue to use non-English Unicode file names, knowing that the document file names will be incorrect in the case package zip file.
- Include only those documents that do not have non-English Unicode file names in the case package.
- Rename the extracted document with the embedded non-English Unicode file name that is listed in the case package PDF.
- Ensure that the third-party utility you use to unzip the case package fully supports UTF-8 format file names.

The file does not open when you click a link to a .zip file in a case package

If you create a case package for a case that includes a .zip file as a case document, the case package PDF contains a link to that .zip file. However, you click on the link in the case package PDF file, the .zip file does not open.

Symptoms

If you click a link to a .zip file in a case package, the file does not open. This problem occurs only for linked case documents that are .zip files. The problem does not occur for linked text, Microsoft Word, or Microsoft Excel documents.

Causes

This problem occurs because of how the Adobe Acrobat Reader handles embedded zipped attachments as documented in the Adobe help page titled *Links and attachments in PDFs* (https://helpx.adobe.com/acrobat/using/links-attachments-pdfs.html).

The following note under "Add an attachment" explains the problem: *If you attach EXE, VBS, or ZIP file formats, Acrobat warns you that it won't open the file once attached because the format is associated with malicious programs, macros, and viruses that can damage your computer.*

Resolving the problem

To open a .zip file in a case package:

- Open the zip file directly. The zip file is included as part of the Case Package and can be opened directly.
- Use Google Chrome browser to open the PDF. The Chrome browser opens the .zip file when you click the link.

Restarting an IBM Content Manager task that fails to start

When an IBM Case Manager task fails to start, you must change the task state manually and restart the task.

Symptoms

Tasks in the case type do not start when they meet the preconditions that were defined for them to start.

Resolving the problem

To restart tasks that failed to start, you must first put these tasks into a state where they can be restarted. Then, you can restart the tasks.

Process Engine or workflow system tasks

To put Process Engine or workflow system tasks that failed into a state where they can be restarted:

1. Open Administration Console for Content Platform Engine, click **Object Stores** and select your target object store.
2. Click **Search** and select **New Object Store Search**.
3. In the **Class** list, select **Task**.
4. In the **Column** list of the **Criteria** section for row A, select **Task State**.
5. In the **Condition** list, select **Equals To**.
6. Enter 6 in the **Value** column.

7. In the **Column** list of the **Criteria** section for row B, select **Last Failure Reason**.
8. In the **Condition** list, select **Equals To**.
9. Enter `CmAcmError Launch Failed` in the **Value** column.
10. In the **Properties** list, select * (asterisk).
11. Click the **Bulk Actions** tab and select **Enable**, then scroll down and select **Run Script**.
12. Enter the following script:

```
function OnCustomProcess (CEObject)
          {
             CEObject.changeState(4194304);
             CEObject.save(1);
          }
```

13. Click **Run** to run the query and the script.

Now that the tasks are in a state where they can be restarted, you can restart the tasks. To restart tasks in IBM Case Manager, you must use the Case REST API. You restart the task by issuing a Restart call to the Case REST API in Poster. For example, issue a Restart call to the Case REST API with the PUT method by using the Poster AddOn for Mozilla Firefox.

The Case REST API checks the task attributes to ensure that the task is in a state from which it can be restarted. For example, you cannot restart a task that is in working state or a task that has exception other than failed to launch.

Important: Some task types cannot be restarted and specific conditions must apply. When the action is set to restart, the task cannot be one of the following task types:

- Container or Compound Task
- IBM Business Process Manager Task
- Discretionary Task

In addition, one of the following conditions must be true:

- The Content Platform Engine workflow item process completed (the value of the `TaskState` property is `Completed`).
- The Content Platform Engine workflow item process failed to launch (the value of the `TaskState` property is `Failed` and the value of the `LastFailureReason` property is `CmAcmError Launch Failed`).
- The Content Platform Engine workflow item process failed and then stopped (the value of the `TaskState` property is `Failed`, the value of the `TaskDisabledState` property is `disabled_aborted`, and the value of the `LastFailureReason` property is set to a Process Engine error).
- The Content Platform Engine workflow item process was running and then stopped (the value of the `TaskState` property is `Failed`, the value of the `TaskDisabledState` property is `disabled_aborted`, and no value is set for the `LastFailureReason` property).

Issue a restart call to the Case REST API with the PUT method by using the Poster AddOn for Mozilla Firefox. Enter the following parameter values in the Request form:

URL:

1. Use a tool like the Firebug Console to find a Request URL like the following example:<PROTOCOL>://<HOST_NAME>:<PORT_NUMBER>/CaseManager/CASEREST/v1/case/993D3E31-EB4E-4646-B879-2A56055BA874?tasks?TargetObjectStore=MyExampleObjectStore&Grouping=ROD
2. When you load the **Tasks** tab for a case, extract the TaskId value from the JSON Response payload for the task that wants to restart. For example, TaskId==7A75A997-0E42-406E-AZC4-EE55D7DER9PF.
3. Use this task ID to build the URL for your restart Request payload. For example, <PROTOCOL>://<HOST_NAME>:<PORT_NUMBER>/CaseManager/CASEREST/v1/task/7A75A997-0E42-406E-AZC4-EE55D7DER9PF?TargetObjectStore=MyExampleObjectStore&Grouping=ROD
4. Enter the URL for your request in the **URL** field in Poster.

Important: The **TargetObjectStore** query string parameter in the URL represents the symbolic name of the Target Object Store. The **Grouping** parameter is a predefined grouping identifier in which the only valid value is **ROD** for Required, Optional, Disabled.

Actions: The Case REST API must be run by using the PUT method.

Content Type: The Content Type of the payload must be **application/json; charset=UTF-8**

Content: The Case REST API to restart the task has a payload like: { "Action" : "restart" }

Box Collaboration action fails in a distributed environment when the date/time is not synchronized

In a distributed or cluster environment, an attempt to perform a Box collaboration action in Case Manager Client fails if system time is not synchronized with the internet time.

Symptoms

You attempt to perform a Box collaboration action such as creating a Box collaboration folder in Case Manager Client. However, the action fails and returns error FNRPA0791E that states that the current date/time is later than the expiration date/time in the “exp” claim.

Resolving the problem

Synchronize the system time on your IBM Case Manager server with the internet time. For instructions on synchronizing the time, refer to the operating system documentation.

Configuring and administering IBM Case Manager from the command line

You can configure and administer IBM Case Manager from the command line instead of using the configuration tool and administration client user interfaces. You can generate tasks, run tasks, list the tasks in a profile, add passwords to task files, move or remove a task, and run a test on some tasks.

Before you begin

Ensure that you have granted file and directory permissions to *config_client_user*, which is the user who runs the configuration tool, to allow this user to run the program and create files in the *install_path*/configure directory.

"Configuring and administering IBM Case Manager from the command line"

"Configuring IBM Case Manager from the command line"

"Command syntax" on page 315

Related tasks:

Granting directory permissions to the administration client user

Configuring and administering IBM Case Manager from the command line

You can configure and administer IBM Case Manager from the command line instead of using the configuration tool and administration client user interfaces. You can generate tasks, run tasks, list the tasks in a profile, add passwords to task files, move or remove a task, and run a test on some tasks.

Before you begin

Ensure that you have granted file and directory permissions to *config_client_user*, which is the user who runs the configuration tool, to allow this user to run the program and create files in the *install_path*/configure directory.

"Configuring and administering IBM Case Manager from the command line"

"Configuring IBM Case Manager from the command line"

"Command syntax" on page 315

Related tasks:

Granting directory permissions to the administration client user

Configuring IBM Case Manager from the command line

You must configure IBM Case Manager before you can use it in production. Configuring your system prepares the Case Manager Builder application and the Case Manager Client application for deployment on the application server. After you deploy these applications, you can create, test, manage, deploy, and work with your business solutions.

About this task

Your case management system consists of a development environment for creating and testing case management solutions and a production environment for working with running case management solutions. You must configure both environments.

Configuring the development environment includes configuring Case Manager Builder and Case Manager Client. Configuring the production environment includes configuring Case Manager Client.

You use the IBM Case Manager configuration tool to create a profile for each development environment instance and a profile for each production environment instance. The information for a profile is collected in XML files in the form of properties and values that describe the associated configuration and deployment tasks. Three XML files contain the information that is common to all tasks in the profile, and each configuration task in the profile has one configuration XML file. You must provide values for the profile properties that are specific to each configuration at your site, such as the application server name.

The XML files are stored in a directory that is unique to a profile. Because the profile name is used for the directory name and for the configuration profile file name, you must provide a profile name that is a valid directory name for your operating system. By default, the profiles are stored in the *install_path*/`configure/profiles` directory where *install_path* is the location where IBM Case Manager is installed. For AIX, Linux, and Linux for System z, the default location is the `/opt/IBM/CaseManagement` directory. For Windows, the default location is the `C:\Program Files\IBM\CaseManagement` directory for a fresh install or the `C:\Program Files (x86)\IBM\CaseManagement` directory for an upgrade. After you create the profile, you must edit the values in the tasks and then apply the settings by running each configuration task.

"Configuring the development environment by using the command line" on page 255

"Importing profile properties by using the command line" on page 263

"Adding users to the default project area by using the command line" on page 271

"Configuring the production environment by using the command line" on page 272

"Defining and modifying project areas by using the command line" on page 284

"Creating a list of object store properties and document types by using the command line" on page 290

"Copying an existing solution by using the command line" on page 292

"Creating a solution from a template by using the command line" on page 293

"Converting a solution to a template by using the command line" on page 294

"Exporting a solution package by using the command line" on page 296

"Importing a solution package by using the command line" on page 298

"Importing a solution from a manifest by using the command line" on page 301

"Generating the object store data map by using the command line" on page 302

"Creating and enabling a Case Analyzer store by using the command line" on page 303

"Creating and enabling a case history store by using the command line" on page 305

Configuring the development environment by using the command line

You must configure the development environment before you use IBM Case Manager to create and deploy solutions. You use the development environment to create, modify, and test solutions before you move them into a production environment. You can use the command line to configure the development environment.

Before you begin

Be sure to have your completed configuration checklist available.

About this task

Configuring the development domain includes configuring Case Manager Builder and Case Manager Client. You must create a profile for each development environment instance that you are configuring.

Procedure

To configure the development environment:

1. Change the current directory to the *install_path*/CaseManagement/configure directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the /opt/IBM/CaseManagement directory.
Windows	By default, *install_path* is the C:\Program Files\IBM\CaseManagement directory for a fresh install or the C:\Program Files (x86)\IBM\CaseManagement directory for an upgrade.

2. Generate the development environment profile and XML files by running the following command. Do not enter any line breaks when you enter the command.

```
configmgr_cl generateConfig content_management_type
 -box -deploy deploy_type -db database_type
 -env environment_type
 -profileType developmentenvironment
 -profile myprofile -form form_type
 [-silent] [-force]
```

content_management_type
Specify -box for Box, -cm8 for IBM Content Manager, or -bpm for IBM Business Process Manager.

-deploy *deploy_types*

Specifies the type of deployment. The value must be `standard`, `cluster`, or `nd`. Specify `standard` if you are deploying IBM Case Manager to a stand-alone WebSphere Application Server, which is a server that is not managed or clustered.

Specify `cluster` if you are deploying IBM Case Manager to a WebSphere Application Server cluster.

Specify `nd` if you are deploying IBM Case Manager in a WebSphere Application Server network deployment environment that is managed but not clustered.

This parameter is required when you are generating all the files at the same time.

-db *database_type*
Required only for the `configibmcm` option. This parameter specifies the type of database that IBM Content Manager uses. Choose a valid value from the following options:

Table 21. Valid database_type values

Environment	environment_type value
DB2	`db2`
Microsoft SQL Server	`mssql`
Oracle	`oracle`
Oracle Real Application Clusters (RAC)	`oracle_rac`

-env *environment_type*
Required only when you are generating all the files at the same time or for `deploycaseforms`.

Table 22. Valid environment_type values

Environment	environment_type value
Stand-alone Profile	`standalone`
Deployment Manager Profile	`dmgr`
Managed Profile	`managed`

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*`/CaseManagement/configure/profiles` directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1"` or `/opt/IBM/CaseManagement/configure/profiles/develop1`.
- The full path to the profile input file, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp"` or `/opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp`.

-form *form_type*
Specifies the form type to integrate with IBM Case Manager. If you specify `ibmforms`, IBM Case Manager will be configured to use eForms and IBM Forms. The *form_type* value can be one of the following items:

- eforms
- ibmforms

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

For example, the following command generates all the configuration XML files for a new development environment configuration profile for a standard deployment with IBM Tivoli Directory Server that uses a stand-alone LDAP repository in the *install_path*/CaseManagement/configure/profiles/develop1 directory:

```
configmgr_cl generateConfig
 -deploy standard
 -db db2 -env standalone
 -profileType wasdevelopmentenvironment
 -profile develop1
```

3. Edit the property values in the configuration XML files that you generated:
   a. Use a text editor or XML editor to open one of the configuration XML files that you generated.
   b. Replace each occurrence of ****INSERT VALUE**** with a value that is appropriate for your site. To change the default value to a blank value, replace <value>****INSERT VALUE****</value> with <value />. See the descriptions in the file for more information.

      Important: You are not required to store values for passwords in the file. You can run the **storePasswords** command later to add encrypted passwords to the file before you run the task.
   c. Replace empty values that have the format <value /> with a value that is appropriate for your site. Use the format <value>*my_value*</value>.
   d. Verify that the default values for the remaining properties are correct for your site.
   e. Verify that the task is enabled for each required task. Set the **enabled** attribute value in the <configuration> element to true in any configuration XML file that you edit if you want to run the configuration task. When a task is disabled, the **execute** command skips the task. For example, the registerexternaldataurl.xml file has the **enabled** attribute value in the <configuration> element set to false by default, and the task will be skipped.
   f. Save your edits and close the XML file.
   g. Repeat as needed until you edit all the required files.

Important: You must provide values for all of the entries in the `websphereapplicationserver.xml` or `weblogicapplicationserver.xml` file, the `contentengineserver.xml` file, and the `contentnavigatorserver.xml` file before you can run any of the tasks.

4. Optional: Add encrypted passwords to the XML files by running the **storePasswords** command for the profile.

   Tip: If you do not add passwords to the XML files, you are prompted for the passwords when you run the task for each file.
   For example, the following command stores all the passwords in the profile named myprofile1:

   ```
   configmgr_cl storepasswords -profile myprofile1
   ```

5. Run the task to update the Content Platform Engine client connector files by entering the following command:

   ```
   configmgr_cl execute -task updatecpeclient
    -profile myprofile [-silent] [-force]
   ```

6. Edit the `updatecpeclient.xml` file to set the **`enabled`** attribute value in the <configuration> element to `false`. This setting disables the task so that it does not run again when you run the entire profile.
7. Run all of the tasks in the development profile by using the following command:

   ```
   configmgr_cl execute -profile myprofile
    [-silent] [-force]
   ```

8. Restart the application server.

What to do next

You must add at least one user to the default project area. Users cannot log into Case Manager Builder until they are added to a project area.

"Development environment tasks and files"

Related tasks:

"Importing profile properties by using the command line" on page 263

Configuration checklist

Related reference:

"**generateConfig** command" on page 347

"**execute** command" on page 333

Related information:

Preparing to configure your case management system

Configuring the development environment

Development environment tasks and files:

Creating a configuration profile creates a set of files that contain information about your environment. You can edit the component files and the task files to update or add information before you run the tasks.

Component files

When you create a profile, you specify the arguments for the application server type, and the FileNet P8 Platform and IBM Content Navigator environment. The settings are saved in files that are specific to each component.

Table 23. Component files for a profile

Component	File Name	Description
Application server	`websphereapplicationserver.xml` or `weblogicapplicationserver.xml`	Application server settings that are common to all tasks in the profile. These settings are used when you run any of the tasks for the development environment profile. The properties include the application server installation directory, the administrative user name and password, the port number, cell, and other information about the application server. Each profile contains only one of these files, depending on the application server type.
Content Platform Engine	`contentengineserver.xml`	Content Platform Engine settings that are common to all tasks in the profile. These settings are used when you run any of the tasks for the development environment profile. The properties include the Content Platform Engine domain information, the case management design object store name, and other information about the development environment.
IBM Content Navigator	`contentnavigatorserver.xml`	IBM Content Navigator settings that are common to all tasks in the profile. These settings are used when you run some of the tasks for the development environment profile. The properties include the IBM Content Navigator server installation directory, the administrative user name and password, the port number, cell, and other information about IBM Content Navigator.

Task files

The task files are generated when you create the profile. For command usage, the argument value for each task is the name of the XML file without the file extension, for example, `configbox`.

Table 24. Tasks for a development environment profile

Task	File Name	Description
Configure Box Collaboration	`configbox.xml`	This task is required if you want to enable case workers to use Box to collaborate with external users. This task configures the connection to the Box server.

Table 24. Tasks for a development environment profile (continued)

Task	File Name	Description
Configure the Case Management Object Stores	`configcmos.xml`	This task installs the IBM Case Manager add-ons for the case management design and target object store and creates the required events and subscriptions in Content Platform Engine.
Configure IBM Business Process Manager	`configibmbpm.xml`	This task configures the connection to the IBM Business Process Manager host server. This task is required if you use IBM Business Process Manager as the workflow server for IBM Case Manager.
Configure the IBM Content Manager Host Properties	`configibmcm.xml`	This task configures the IBM Case Manager integration with IBM Content Manager.
Configure Business Rules	`configrules.xml`	This task configures the environment to be able to use rules in solutions. **Tips:** • You can select only one locale in which to write the business rules for your solutions. If you need to create solutions with business rules in other locales, rerun this task to change the rule persistence locale before you create the solution. After the first rule for a solution is saved, the rule persistence locale cannot be changed. • If you rerun this task to change the location of the rules repository directory after you deploy any solutions, complete the following steps after you run the task: 1. Stop Content Platform Engine. 2. From the previous rules repository directory, move the `res_data` directory to the new location of the rules repository directory. In a cluster environment, the rules directory must be a shared directory that can be accessed by all Content Platform Engine cluster servers. 3. Restart Content Platform Engine.
Create Case Manager Applications	`createapps.xml`	This task connects different components in your IBM Case Manager environment. You must run this task before you run the Deploy the Case Manager API WAR task or the Deploy the Forms Application task.

Table 24. Tasks for a development environment profile (continued)

Task	File Name	Description
Define the Default Project Area	`definedefaultprojectarea.xml`	Each development environment requires a default project area to group users and solutions within the design object store for Case Manager Builder. Only users who are assigned to a project area can log into Case Manager Builder.
Deploy the Case Manager API	`deploycaseapi.xml`	This task deploys the IBM Case Manager API application to the application server. Case Manager Builder and Case Manager Client use the IBM Case Manager API application to interact with Content Platform Engine.
Deploy the Forms Application	`deploycaseforms.xml`	This task is required if IBM Case Manager integrates with IBM Forms or IBM FileNet P8 eForms. If you configure IBM Forms or IBM FileNet P8 eForms on a network deployment or cluster environment, run this task in the profile that contains the other tasks. Select **Network Deployment** or **Cluster** for the deployment type, **eForms and IBM Forms** for the forms type, and **Deployment Manager Profile** for the environment type. If you integrate with IBM Forms 8.1 or earlier on a network deployment or cluster environment, the following additional steps are required. These additional steps are not required if you integrate with IBM Forms 8.2 or later or with only IBM FileNet P8 eForms. 1. For the managed nodes, create a profile on each managed node that includes only this task and run this task. Select **Network Deployment** or **Cluster** for the deployment type, **eForms and IBM Forms** for the forms type, and **Managed Profile** for the environment type. 2. After all nodes are configured, the managed node or cluster must be restarted to complete the forms integration. You can restart the managed node or cluster now, or after you run all other configuration tasks.

Table 24. Tasks for a development environment profile (continued)

Task	File Name	Description
Deploy Case Manager Builder	`deploycmbapp.xml`	This task deploys the Case Manager Builder EAR file to the application server. Deploying the EAR file makes the Case Manager Builder application available for users to log in.
Deploy the IBM Business Process Manager Integration Service	`deployibmbpmis.xml`	The IBM Business Process Manager integration service provides immediate workflow status to the IBM Case Manager server. This task configures the communication between the Content Platform Engine server and the IBM Business Process Manager server.
Deploy and Register Extensions Package	`deployregisterextensions.xml`	This task registers and deploys your extensions package.
Deploy and Register Widgets Package	`deployregisterwidgets.xml`	This task registers the widgets package with the IBM Case Manager server, registers the plug-in for the widgets package with the IBM Content Navigator server, and deploys the EAR file in the widgets package to the web application server. This task is required for the default widgets package that comes with IBM Case Manager. You can also run this task to register your custom widgets packages.
Register the IBM Case Manager Administration Client Plug-in	`registeradmin.xml`	This task registers the plug-in for IBM Content Navigator that contains the administration client for IBM Case Manager. This task is required. Save your changes and run the task to apply your settings.
Register the IBM Case Manager Box Event Listener Plug-in	`registerboxlistener.xml`	This task registers the plug-in for IBM Content Navigator that listens for case-related Box events when Box collaboration is enabled. This task is required if you want Box events to trigger the creation of cases or work items. Save your changes and run the task to apply your settings.
Register the IBM Content Platform Engine Applets Support Plug-in	`registercpeapplets.xml`	This task registers the plug-in for IBM Content Navigator that contains the Process Designer applet.
Register the External Data Service	`registerexternaldataurl.xml`	This task creates a connection to an external data service, which allows you to use data in a solution from a source other than Content Platform Engine.

Table 24. Tasks for a development environment profile (continued)

Task	File Name	Description
Register the Case Monitor Widgets Package	`registericmmonitor.xml`	This task imports and registers the Case Monitor widgets package with the IBM Case Manager server, registers the plug-in for the widgets package with the IBM Content Navigator server, and creates the Case Monitor desktop. This task is required to enable Case Monitor. Save your changes and run the task to apply your settings. In a cluster environment, you must either use the IBM Content Navigator administration client to manually load the plug-in inside of the extensions package on each node or restart the application server cluster to force all nodes to load the plug-in. Before using Case Monitor, you must create a Case Analyzer store for each case management target object store.
Register the Project Area	`registerprojectarea.xml`	This task registers a project area with an IBM Case Manager desktop, creates default IBM Case Manager desktops, configures repositories for the case management design and target object stores, and adds IBM Case Manager features to the desktop. Also, this task configures the Case Operations component queue and configures the project area's isolated region to work with solution workflows. This task is required and must be run for every project area.
Register the IBM Case Manager Services Plug-in	`registerservices.xml`	This task registers the plug-in for IBM Content Navigator that contains the IBM Case Manager services that are used by other components.
Update the Content Platform Engine Client Connector Files	`updatecpeclient.xml`	This task connects to the Content Platform Engine server to download and install updated client connector files. Run this task and restart the configuration tool before you run any of the other tasks.

Importing profile properties by using the command line

You can import properties values from an existing configuration profile into the currently opened profile by using the command line. Importing existing values saves time when you are reusing information across profiles.

About this task

Importing properties also provides a way to reuse values from an IBM Case Manager version 5.2.1 or version 5.3.0 configuration profile. For example, you can

import an IBM Case Manager version 5.2.1 or version 5.3.0 development environment profile into a IBM Case Manager version 5.3.1 WebSphere development environment profile.

When you select a profile to import from, the values in the profile are compared with the currently open profile. If the source profile contains all default values for a specific task, nothing is imported for that task. If the target task type supports multiple files of that type, a new task file will be created for the imported values. For example, if both the source and target `configureldap.xml` files contain nondefault values, a new `configureldap.`*`n`*`.xml` file is created for the imported values.

For a list of IBM Case Manager version 5.2.1 tasks, see the following topics:

- Configuring the upgraded development environment
- Configuring the upgraded test or production environment

For a list of IBM Case Manager version 5.3.0 tasks, see the following topics:

- Configuring the upgraded development environment
- Configuring the upgraded test or production environment

Restriction: You can import values only from compatible task types.

Tip: You can run the **listImportTargetTasks** command for more information about legal values for arguments.

Procedure

To import profile properties:

1. Change the current directory to the *`install_path`*`/CaseManagement/configure` directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the `/opt/IBM/CaseManagement` directory.
Windows	By default, *install_path* is the `C:\Program Files\IBM\CaseManagement` directory for a fresh install or the `C:\Program Files (x86)\IBM\CaseManagement` directory for an upgrade.

2. Import the values from a single XML configuration file by running the following command. Do not enter any line breaks when you enter the command:

```
configmgr_cl importProps  -source source_profile
 -sourceTask task_type | -sourceTaskName task_name
 -target target_profile
 -targetTask task_type | -targetTaskName task_name
 [-silent] [-force] [-help]
```

`-source` ***`source_profile`***
Specifies the full path to the directory where the source profile is located. Property values will be imported from this profile. If the path includes a directory name with spaces, enclose the entire path in double quotation marks. For example, enter `"C:\Program Files\profiles\develop1"`.

`-sourceTask` ***`task_type`***

Specifies the type of task that you want to import values from. If you specify the **sourceTask** *task_type* parameter, you can omit the **-sourceTaskName** *task_type* parameter.

Table 25. Valid task_type and task_name values

Task type option	Default task display name	Description
`configcaseloginmodules`	Configure the Login Modules	Imports the properties from the task that configures the login modules for the Case Manager Builder application. The login modules provide authentication information for the Case Manager Builder application. The properties are stored in the `configcaseloginmodules.xml` file.
`configbox`	Configure Box Collaboration	This task is required if you want to enable case workers to use Box to collaborate with external users. This task configures the connection to the Box server.
`configcmos`	Configure the Case Management Object Stores	Imports the properties from the task that configures the development environment design and target object stores. This task installs the IBM Case Manager Add-ons and creates the required events and subscriptions in Content Engine. The properties are stored in the `configcmos.xml` file.
`configibmbpm`	Configure IBM Business Process Manager	Imports the properties from the task that configures the connection to the IBM Business Process Manager host server. This task is required if you use IBM Business Process Manager as the workflow server for IBM Case Manager.
`configibmcm`	Configure IBM Content Manager	This task configures the connection to the IBM Content Manager host server. This task is required if you use IBM Content Manager as the content repository for IBM Case Manager.
`configrules`	Configure Business Rules	Imports the properties from the task that configures Business Rules for your environment and configures the Rules Operations component queue. This task is optional. You must run the Register Target Environment task before you run this task.
`configureldap`	Configure LDAP	Imports the properties from the task that configures the directory service provider (LDAP) settings for the Case Manager Builder application. The directory service provider (LDAP) settings define the directory service and the users and groups that uses for authentication. The properties are stored in the following files: `configureldap.xml` `configureldap.`*n*`.xml` . *n* is an integer starting with 2.

Table 25. Valid task_type and task_name values (continued)

Task type option	Default task display name	Description
`contentengineserver`	Content Platform Engine	Content Platform Engine settings that are common to all tasks in the profile. These settings are used when you run any of the tasks for the production environment profile. The properties include the Content Platform Engine domain information, the case management design object store name, and other information about the production environment.
`contentnavigatorserver`	IBM Content Navigator	IBM Content Navigator settings that are common to all tasks in the profile. These settings are used when you run some of the tasks for the production environment profile. The properties include the IBM Content Navigator server installation directory, the administrative user name and password, the port number, cell, and other information about IBM Content Navigator.
`createapps`	Create Case Manager Applications	Imports the properties from the task that adds the Content Platform Engine EJB URL and timeout values to the IBM Case Manager API WAR file, adds the location of the help topics to the IBM Case Manager help system WAR file, and configures the IBM Case Manager Forms WAR file for FileNet eForms or IBM Forms. You must run this task before you run the Deploy the Case Manager API WAR task, the Deploy Case Manager Help System task, or the Deploy the Forms Application task. If you change the location of your network shared directory after you run this task, you must run this task again and redeploy the IBM Case Manager help system WAR file.
`definedefaultprojectarea`	Define the Default Project Area	Imports the properties from the task that defines the default project area for the development environment. A project area groups solutions in the design object store so that the entire object store is not affected when you reset the test environment. Only users who are assigned to a project area can log on to Case Manager Builder. The default project area is required for each development environment.
`definetargetenv`	Define Target Environment	Imports the properties from the task that defines a target environment for the production environment. A case management solution is deployed to a target environment. A target environment consists of a connection point and an object store, and is associated with one or more IBM Content Navigator desktops. A unique target environment is required for every connection point that will be used for solution deployment. This task is required.

Table 25. Valid task_type and task_name values (continued)

Task type option	Default task display name	Description
`deploycaseapi`	Deploy the IBM Case Manager API	Imports the properties from the task that deploys the IBM Case Manager API application on the web application server. Deploying the IBM Case Manager API application makes the application available for use by the IBM Case Manager application. The properties are stored in the `deploycaseapi.xml` file.
`deploycaseforms`	Deploy the Forms Application	Imports the properties from the task that integrates forms into your case management configuration. This task is required. You must run the Create the Case Manager Applications task before you run this task. If you are integrating with IBM Forms on a stand-alone server, you must restart your application server after you run this task. If you are integrating with IBM Forms on a network deployment or cluster, you must first deploy the application against the deployment manager, run the task against each managed node, then restart your managed node or cluster after running the task on all managed nodes. If you do not use IBM Forms, you are not required to restart the application server.
`deploycmbapp`	Deploy Case Manager Builder	Imports the properties from the task that deploys a Case Manager Builder instance on the web application server. Deploying makes the Case Manager Builder application available for use. The properties are stored in the `deploycmbapp.xml` file.
`deployibmbpmis`	Deploy the IBM Business Process Manager Integration Service	The IBM Business Process Manager integration service provides immediate workflow status to the IBM Case Manager server. This task configures the communication between the Content Platform Engine server and the IBM Business Process Manager server. This task is required if you use IBM Business Process Manager as the workflow server for IBM Case Manager.
`deployregisterextensions`	Deploy and Register Extensions Package	This task registers and deploys your extensions package.
`deployregisterwidgets`	Deploy and Register Widgets Package	Imports the properties from the task that registers the widgets package with the IBM Case Manager server, registers the plug-in for the widgets package with the IBM Content Navigator server, and deploys the EAR file in the widgets package to the web application server, if present. This task is required for the default widgets package that comes with IBM Case Manager. You can also run this task to register your custom widgets packages.

Table 25. Valid task_type and task_name values (continued)

Task type option	Default task display name	Description
`deploysolution`	Deploy Solution	Imports the properties from the task that deploys an IBM Case Manager solution into a production target object store. The properties are stored in the following files: `deploysolution.xml` `deploysolution.`*n*`.xml`. *n* is an integer starting with 2.
`registerboxlistener`	Register the IBM Case Manager Box Event Listener Plug-in	This task registers the plug-in for IBM Content Navigator that listens for case-related Box events when Box collaboration is enabled. This task is required if you want Box events to trigger the creation of cases or work items. Save your changes and run the task to apply your settings.
`registercpeapplets`	Register the IBM Content Platform Engine Applets Support Plug-in	This task registers the plug-in for IBM Content Navigator that contains the Process Designer applet.
`registerexternaldataurl`	Register the External Data Service	This task creates a connection to an external data service, which allows you to use data in a solution from a source other than Content Platform Engine. This task is required only if you are using an external data service in a solution.
`registerprojectarea`	Register Project Area	Imports the properties from the task registers a project area with an IBM Content Navigator desktop, creates the default IBM Case Manager desktops, configures the repositories for the case management design and target object stores, and adds IBM Case Manager features to the desktop. Also, this task configures the Case Operations component queue and configures the project area's isolated region to work with solution workflows. This task is required and must be run for every project area. You must run the Deploy and Register Widgets Package task and the Register the IBM Case Manager Administration Client Plug-in task before you run this task.
`registerservices`	Register the IBM Case Manager Services Plug-in	Imports the properties from the task that registers the plug-in for IBM Content Navigator that contains the IBM Case Manager services that are used by other components. This task is required.

Table 25. Valid task_type and task_name values (continued)

Task type option	Default task display name	Description
`registertargetenv`	Register Target Environment	Imports the properties from the task registers a target environment with an IIBM Content Navigator desktop, creates the default IBM Case Manager desktops, configures the repositories for the case management design and target object stores, and adds IBM Case Manager features to the desktop. Also, this task configures the Case Operations component queue and configures the target environment's isolated region to work with solution workflows. This task is required and must be run for every target environment. You must run the Deploy and Register Widgets Package task and the Register the IBM Case Manager Administration Client Plug-in task before you run this task.
`updatecpeclient`	Update the Content Platform Engine Client Connector files	Imports the properties from the task that downloads the correct version of the Content Platform Engine Client Connector files.
`websphereapplicationserver` or `weblogicapplicationserver`	Application server	Application server settings that are common to all tasks in the profile. These settings are used when you run any of the tasks for the production environment profile. The properties include the application server installation directory, the administrative user name and password, the port number, cell, and other information about the application server. Each profile contains only one of these files, depending on the application server type.
`registericmmonitor`	Register the Case Monitor Widgets Package	This task imports and registers the Case Monitor widgets package with the IBM Case Manager server, registers the plug-in for the widgets package with the IBM Content Navigator server, and creates the Case Monitor desktop. This task is required to enable Case Monitor. Save your changes and run the task to apply your settings. In a cluster environment, you must either use the IBM Content Navigator administration client to manually load the plug-in inside of the extensions package on each node or restart the application server cluster to force all nodes to load the plug-in. Before using Case Monitor, you must create a Case Analyzer store for each case management target object store.

`-sourceTaskName` ***`task_name`***

Specifies the display name for the task that you want to import values from. If you specify the **`sourceTask`** *task_type* parameter, you can omit the **`-sourceTaskName`** *task_type* parameter.

If the display name includes spaces, you must use quotation marks around the display name, as in the following example:

```
-sourceTaskName "Configure LDAP"
```

-target *target_profile*
Specifies the full path to the directory where the target profile is located. The values will be imported into this profile.

-targetTask *task_type*

Specifies the type of task that you want to import values to. If you specify the **targetTask** *task_type* parameter, you can omit the **-targetTaskName** *task_type* parameter.

See the "Valid task_type and task_name values" table for a list of valid *task_type* values.

-targetTaskName *task_name*

Specifies the display name for the task that you want to import values to. If you specify the **targetTask** *task_type* parameter, you can omit the **-targetTaskName** *task_type* parameter.

See the "Valid task_type and task_name values" table for a list of valid *task_name* values.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

For example, the following command imports the properties for the Configure LDAP task from the develop1 profile into the Configure LDAP task for the wasdevelop1 profile:

```
configmgr_cl  importProps
 -source
"C:\Program Files (x86)\IBM\CaseManagement\configure\profiles\develop1"
 -sourceTask configureldap
 -target
"C:\Program Files (x86)\IBM\CaseManagement\configure\profiles\wasdevelop1"
 -targetTask configureldap
```

Related tasks:

Importing profile properties

Related reference:

"**listImportTargetTasks** command" on page 380

Adding users to the default project area by using the command line

You must add at least one user to the default project area. Users cannot log into Case Manager Builder until they are added to a project area.

Before you begin

Be sure to have your completed configuration checklist available.

About this task

A project area groups solutions within the design object store to limit the effects of resetting the test environment. When you reset the test environment from Case Manager Builder, only a single project area is reset. Each development environment has a default project area, and you can create more project areas as needed to provide isolated work areas for developing and testing solutions in Case Manager Builder. The default project area is named dev_env_connection_definition.

Before you add users to the project area, add them to the master group that you configured for access to your object store.

You can assign specific solutions and users to each project area. Each user can belong only to one project area and the default project area. If you assigned a user to another project area who is already assigned to any nondefault project area, that user is automatically removed from the original nondefault project area. You can add groups to the default project area only.

Adding a user to a project area gives the user access to the solutions in the project area in the design object store. If the user is not an administrator for the target object store, then you must set the security for the user.

By default, all new solutions are created in the default project area unless you define additional project areas.

Procedure

To add users to the default project area:

1. Change the current directory to the *install_path*/CaseManagement/configure directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the /opt/IBM/CaseManagement directory.
Windows	By default, *install_path* is the C:\Program Files\IBM\CaseManagement directory for a fresh install or the C:\Program Files (x86)\IBM\CaseManagement directory for an upgrade.

2. Add a single user or group by running the following command. Do not enter any line breaks when you enter the command.

```
configmgr_cl addPrincipals -projectAreaName dev_env_connection_definitition
 -profile myprofile
 -user user_name -groups group_name
 [-help]
```

-projectAreaName dev_env_connection_definition
The name of the project area to modify. The default project area is named dev_env_connection_definitition.

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-user *user_name*
Specifies the short name or display name of the user to add. A user can belong to the default project area and one other project area.

-groups *group_name*
Specifies the short name or display name of the group to add. Groups can be added to the default project area only.

-help
Optional and displays a brief message on the command syntax instead of running the command.

3. Repeat 2 on page 271 as needed to add all the users or groups for the default project area. You will assign solutions to the default project area later, after you create the solutions. You also can create additional project areas and assign users and solutions later.

Related tasks:

"Defining and modifying project areas by using the command line" on page 284

Configuration checklist

Configuring the production environment by using the command line

You must configure the production environment before you deploy your solutions to that production environment. You configure the production environment after you configure the development environment. You can use the command line to configure the production environment.

Before you begin

Be sure to have your completed configuration checklist available.

About this task

Configuring the production domain includes configuring Case Manager Client.

Procedure

To configure the production environment:

1. Change the current directory to the *install_path*/CaseManagement/configure directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the /opt/IBM/CaseManagement directory.
Windows	By default, *install_path* is the C:\Program Files\IBM\CaseManagement directory for a fresh install or the C:\Program Files (x86)\IBM\CaseManagement directory for an upgrade.

2. Generate the production environment profile and XML files by running the following command. Do not enter any line breaks when you enter the command:

```
configmgr_cl generateConfig content_management_type
 -deploy deploy_type -db database_type
 -env environment_type
 -profileType production_environment
 -profile myprofile -form form_type
 [-silent] [-force]
```

content_management_type
Specify one of the following values:

- -box for Box
- -bpm for IBM Business Process Manager
- -cm8 for IBM Content Manager

-deploy *deploy_types*

Specifies the type of deployment. The value must be standard, cluster, or nd. Specify standard if you are deploying IBM Case Manager to a stand-alone WebSphere Application Server, which is a server that is not managed or clustered.

Specify cluster if you are deploying IBM Case Manager to a WebSphere Application Server cluster.

Specify nd if you are deploying IBM Case Manager in a WebSphere Application Server network deployment environment that is managed but not clustered.

This parameter is required when you are generating all the files at the same time.

-db *database_type*
Required only for the configibmcm option. This parameter specifies the type of database that IBM Content Manager uses. Choose a valid value from the following options:

Table 26. Valid database_type values

Environment	environment_type value
DB2	db2
Microsoft SQL Server	mssql
Oracle	oracle
Oracle Real Application Clusters (RAC)	oracle_rac

-env *environment_type*

Required only when you are generating all the files at the same time. This parameter specifies the type of environment that the WebSphere Application Server profile uses.

Table 27. Valid environment_type values

Environment	environment_type value
Stand-alone Profile	`stand-alone`
Deployment Manager Profile	`dmgr`
Managed Profile	`managed`

-profileType *production_environment*

This parameter specifies the type of profile. Use one of the following values:

Table 28. Valid production_environment values

Environment	production_environment value
WebSphere Application Server	`wasproductionenvironment`
Oracle WebLogic Server	`wlproductionenvironment`

-profile *myprofile*

Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*`/CaseManagement/configure/profiles` directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1"` or `/opt/IBM/CaseManagement/configure/profiles/develop1`.
- The full path to the profile input file, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp"` or `/opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp`.

-form *form_type*

Specifies the form type to integrate with IBM Case Manager. If you specify `ibmforms`, IBM Case Manager will be configured to use eForms and IBM Forms. The *form_type* value can be one of the following items:

- `eforms`
- `ibmforms`

-silent

Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force

Optional and applies only when the **-silent** parameter is used. When you

specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

For example, the following command generates all the configuration XML files for a new WebSphere Application Server production environment configuration profile for a standard deployment with IBM Tivoli Directory Server that uses a stand-alone LDAP repository in the *install_path*/CaseManagement/configure/profiles/production1 directory:

```
configmgr_cl generateConfig
 -deploy standard
 -db db2 -env standalone
 -profileType wasproductionenvironment
 -profile production1
```

3. Edit the property values in the configuration XML files that you generated:
   a. Use a text editor or XML editor to open one of the configuration XML files that you generated.
   b. Replace each occurrence of ****INSERT VALUE**** with a value that is appropriate for your site. To change the default value to a blank value, replace <value>****INSERT VALUE****</value> with <value />. See the descriptions in the file for more information.

      Important: You are not required to store values for passwords in the file. You can run the **storePasswords** command later to add encrypted passwords to the file before you run the task.
   c. Replace empty values that have the format <value /> with a value appropriate for your site. Use the format <value>*my_value*</value>.
   d. Verify that the default values for the remaining properties are correct for your site.
   e. Verify that the task is enabled for each required task. Set the **enabled** attribute value in the <configuration> element to true in any configuration XML file that you edit if you want to run the configuration task. When a task is disabled, the **execute** command skips the task. For example, the registerexternaldatauri.xml file has the **enabled** attribute value in the <configuration> element set to false by default, and the task will be skipped.
   f. Save your edits and close the XML file.
   g. Repeat as needed until you edit all the required files.

      Important: You must provide values for all of the entries in the websphereapplicationserver.xml or weblogicapplicationserver.xml file, the contentengineserver.xml file, and the contentnavigatorserver.xml file before you can run any of the tasks.
4. Optional: Add encrypted passwords to the XML files by running the **storePasswords** command for the profile.

   Tip: If you do not add passwords to the XML files, you are prompted for the passwords when you run the task for each file.
   For example, the following command stores all the passwords in the profile named myprofile1:

   ```
   configmgr_cl storePasswords -profile myprofile1
   ```
5. Run the task to update the Content Platform Engine client connector files by entering the following command:

```
configmgr_cl execute -task updatecpeclient
 -profile myprofile [-silent] [-force]
```

6. Edit the `updatecpeclient.xml` file to set the **enabled** attribute value in the <configuration> element to `false`. This setting disables the task so that it does not run again when you run the entire profile.
7. Run all of the tasks in the production profile by using the following command:

```
configmgr_cl execute -profile myprofile
 [-silent] [-force]
```

8. Restart the application server.

"Production environment tasks and files"

"Configuring additional object stores for the production environment by using the command line" on page 281

Related tasks:

"Importing profile properties by using the command line" on page 263

Configuring the production environment

Related reference:

"**generateConfig** command" on page 347

"**execute** command" on page 333

Related information:

Preparing to configure your case management system

Production environment tasks and files:

Creating a configuration profile creates a set of files that contain information about your environment. You can edit the component files and the task files to update or add information before you run the tasks.

Component files

When you create a profile, you specify the arguments for the application server type, and the FileNet P8 Platform and IBM Content Navigator environment. The settings are saved in files that are specific to each component.

Table 29. Component files for a profile

Component	File Name	Description
Application server	`websphereapplicationserver.xml` or `weblogicapplicationserver.xml`	Application server settings that are common to all tasks in the profile. These settings are used when you run any of the tasks for the production environment profile. The properties include the application server installation directory, the administrative user name and password, the port number, cell, and other information about the application server. Each profile contains only one of these files, depending on the application server type.

Table 29. Component files for a profile (continued)

Component	File Name	Description
Content Platform Engine	`contentengineserver.xml`	Content Platform Engine settings that are common to all tasks in the profile. These settings are used when you run any of the tasks for the production environment profile. The properties include the Content Platform Engine domain information, the case management staging object store name, and other information about the production environment.
IBM Content Navigator	`contentnavigatorserver.xml`	IBM Content Navigator settings that are common to all tasks in the profile. These settings are used when you run some of the tasks for the production environment profile. The properties include the IBM Content Navigator server installation directory, the administrative user name and password, the port number, cell, and other information about IBM Content Navigator.

Task files

The task files are generated when you create the profile. For command usage, the argument value for each task is the name of the XML file without the file extension, for example, `configbox`.

Table 30. Tasks for a development environment profile

Task	File Name	Description
Configure Box Collaboration	`configbox.xml`	This task is required if you want to enable case workers to use Box to collaborate with external users. This task configures the connection to the Box server.
Configure the Case Management Object Stores	`configcmos.xml`	This task installs the IBM Case Manager add-ons for the case management staging and target object store and creates the required events and subscriptions in Content Platform Engine.
Configure IBM Business Process Manager	`configibmbpm.xml`	This task configures the connection to the IBM Business Process Manager host server. This task is required if you use IBM Business Process Manager as the workflow server for IBM Case Manager.
Configure the IBM Content Manager Host Properties	`configibmcm.xml`	This task configures the IBM Case Manager integration with IBM Content Manager.

Table 30. Tasks for a development environment profile (continued)

Task	File Name	Description
Configure Business Rules	`configrules.xml`	This task configures the environment to be able to use rules in solutions. **Tips:** • You can select only one locale in which to write the business rules for your solutions. If you need to create solutions with business rules in other locales, rerun this task to change the rule persistence locale before you create the solution. After the first rule for a solution is saved, the rule persistence locale cannot be changed. • If you rerun this task to change the location of the rules repository directory after you deploy any solutions, complete the following steps after you run the task: 1. Stop Content Platform Engine. 2. From the previous rules repository directory, move the `res_data` directory to the new location of the rules repository directory. In a cluster environment, the rules directory must be a shared directory that can be accessed by all Content Platform Engine cluster servers. 3. Restart Content Platform Engine.
Create Case Manager Applications	`createapps.xml`	This task connects different components in your IBM Case Manager environment. You must run this task before you run the Deploy the Case Manager API WAR task or the Deploy the Forms Application task.
Define the Target Environment	`definetargetenv.xml`	A case management solution is deployed to a target environment. A target environment consists of a connection point and an object store, and is associated with one or more IBM Content Navigator desktops. A unique target environment is required for every connection point that will be used for solution deployment.
Deploy the Case Manager API	`deploycaseapi.xml`	This task deploys the IBM Case Manager API application to the application server. Case Manager Builder and Case Manager Client use the IBM Case Manager API application to interact with Content Platform Engine.

Table 30. Tasks for a development environment profile (continued)

Task	File Name	Description
Deploy the Forms Application	`deploycaseforms.xml`	This task is required if IBM Case Manager integrates with IBM Forms or IBM FileNet P8 eForms. If you configure IBM Forms or IBM FileNet P8 eForms on a network deployment or cluster environment, run this task in the profile that contains the other tasks. Select **Network Deployment** or **Cluster** for the deployment type, **eForms and IBM Forms** for the forms type, and **Deployment Manager Profile** for the environment type. If you integrate with IBM Forms 8.1 or earlier on a network deployment or cluster environment, the following additional steps are required. These additional steps are not required if you integrate with IBM Forms 8.2 or later or with only IBM FileNet P8 eForms. 1. For the managed nodes, create a profile on each managed node that includes only this task and run this task. Select **Network Deployment** or **Cluster** for the deployment type, **eForms and IBM Forms** for the forms type, and **Managed Profile** for the environment type. 2. After all nodes are configured, the managed node or cluster must be restarted to complete the forms integration. You can restart the managed node or cluster now, or after you run all other configuration tasks.
Deploy the IBM Business Process Manager Integration service	`deployibmbpmis.xml`	The IBM Business Process Manager integration service provides immediate workflow status to the IBM Case Manager server. This task configures the communication between the Content Platform Engine server and the IBM Business Process Manager server.
Deploy and Register Extensions Package	`deployregisterextensions.xml`	This task registers and deploys your extensions package.

Table 30. Tasks for a development environment profile (continued)

Task	File Name	Description
Deploy and Register Widgets Package	`deployregisterwidgets.xml`	This task registers the widgets package with the IBM Case Manager server, registers the plug-in for the widgets package with the IBM Content Navigator server, and deploys the EAR file in the widgets package to the web application server. This task is required for the default widgets package that comes with IBM Case Manager. You can also run this task to register your custom widgets packages.
Deploy Solution	`deploysolution.xml`	This task deploys a case management solution to a production environment object store. After you deploy the solution, users can log on to Case Manager Client to create cases and work items, view and edit case data, and complete work items for a case. This task is required for each solution that you deploy to your production environment.
Register the IBM Case Manager Administration Client Plug-in	`registeradmin.xml`	This task registers the plug-in for IBM Content Navigator that contains the administration client for IBM Case Manager. This task is required. Save your changes and run the task to apply your settings.
Register the IBM Case Manager Box Event Listener Plug-in	`registerboxlistener.xml`	This task registers the plug-in for IBM Content Navigator that listens for case-related Box events when Box collaboration is enabled. This task is required if you want Box events to trigger the creation of cases or work items. Save your changes and run the task to apply your settings.
Register the External Data Service	`registerexternaldataurl.xml`	This task creates a connection to an external data service, which allows you to use data in a solution from a source other than Content Platform Engine.

Table 30. Tasks for a development environment profile (continued)

Task	File Name	Description
Register the Case Monitor Widgets Package	`registericmmonitor.xml`	This task imports and registers the Case Monitor widgets package with the IBM Case Manager server, registers the plug-in for the widgets package with the IBM Content Navigator server, and creates the Case Monitor desktop. This task is required to enable Case Monitor. Save your changes and run the task to apply your settings. In a cluster environment, you must either use the IBM Content Navigator administration client to manually load the plug-in inside of the extensions package on each node or restart the application server cluster to force all nodes to load the plug-in. Before using Case Monitor, you must create a Case Analyzer store for each case management target object store.
Register the IBM Case Manager Services Plug-in	`registerservices.xml`	This task registers the plug-in for IBM Content Navigator that contains the IBM Case Manager services that are used by other components.
Register Target Environment	`registertargetenv.xml`	This task registers a target environment with an IBM Content Navigator desktop, creates default IBM Case Manager desktops, configures repositories for the case management staging and target object stores, and adds IBM Case Manager features to the desktop. Also, this task configures the Case Operations component queue and configures the target environment's isolated region to work with solution workflows.
Update the Content Platform Engine Client Connector Files	`updatecpeclient.xml`	This task connects to the Content Platform Engine server to download and install updated client connector files. Run this task and restart the configuration tool before you run any of the other tasks.

Configuring additional object stores for the production environment by using the command line:

You must configure the case management object store for each object store in your production environment. You can create a new configuration XML file for each object store and use the command line to run the task.

Before you begin

Be sure to have your completed configuration checklist available.

About this task

You must edit and run the configuration XML file for each object store. The `configcmos.xml` XML file was created when you generated the development environment profile files. You must create and run one additional `configcmos.n.xml` file for each object store in your production environment.

Procedure

To configure multiple object stores:

1. Change the current directory to the *install_path*`/CaseManagement/configure` directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the `/opt/IBM/CaseManagement` directory.
Windows	By default, *install_path* is the `C:\Program Files\IBM\CaseManagement` directory for a fresh install or the `C:\Program Files (x86)\IBM\CaseManagement` directory for an upgrade.

2. If you have more than one object store in your production environment, generate an additional `configcmos.n.xml` file by running the following command. Do not type any line breaks when you enter the command:

```
configmgr_cl generateConfig
 -task configcmos
 -profile myprofile
 [-silent] [-force]
```

where

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*`/CaseManagement/configure/profiles` directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1"` or `/opt/IBM/CaseManagement/configure/profiles/develop1`.
- The full path to the profile input file, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp"` or `/opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp`.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you

specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

For example, the following command generates one `configcmos.n.xml` file for the existing production environment profile that is named Production1:

```
configmgr_cl generateConfig
 -task configcmos
 -profile Production1
```

3. Repeat 2 on page 282 as needed for each object store. The file name increments for each new file that you generate.
4. Edit the property values in the `configcmos.n.xml` files that you generated:
   a. Use a text editor or XML editor to open one of the configuration XML files that you generated.
   b. Replace each occurrence of `****INSERT VALUE****` with a value appropriate for your site. See the descriptions in the file for more information and use your configuration checklists.

      Important: You are not required to store values for passwords in the file. You can run the **storePasswords** command later to add encrypted passwords to the file.
   c. Replace empty values that have the format `<value />` with a value appropriate for your site. Use the format `<value>my_value</value>`.
   d. Verify that the default values for the remaining properties are correct for your site.
   e. Set the **enabled** attribute value in the <configuration> tag to `true` in any configuration XML file that you edit if you want to run the configuration task. When a task is disabled, the **execute** command skips the task.
   f. Save your edits and close the XML file.
   g. Repeat as needed until you edit all the `configcmos.n.xml` files for your profile.
5. Run the `configcmos` tasks in the profile one at a time by running the following command. Do not type any line breaks when you enter the command:

   ```
   configmgr_cl execute -taskfile task_file_name
    -profile myprofile [-silent] [-force]
   ```

   task_file_name is the name of the task file, `configcmos.n.xml`, and *n* is a number larger than 2.
6. Repeat 5 as needed for each object store that you generated a task file for.

What to do next

Additional steps are required to set up a target environment to use the new target object store.

Related tasks:

"Setting up target environments" on page 54

Related reference:

"**generateConfig** command" on page 347

"**execute** command" on page 333

Defining and modifying project areas by using the command line

You use project areas to limit the effects of resetting the test environment. You can define new project areas, define a default project area, assign solutions and users to a project area, and remove project areas by using the command line.

About this task

Each development environment requires a default project area that is named dev_env_connection_definition. However, you can define more project areas as needed. Because you might have multiple people working in the development environment on multiple projects, you can define project areas to limit the effects of resetting the test environment. When you reset the test environment from Case Manager Builder, only a single project area is reset. The entire object store is not affected, and other users can continue working without interruption.

"Defining a project area by using the command line"

"Adding users to a project area by using the command line" on page 286

"Adding solutions to a project area by using the command line" on page 288

Related tasks:

"Defining project areas" on page 52

Related reference:

"**modifyProjectArea** command" on page 397

"**deleteProjectArea** command" on page 332

"**removePrincipals** command" on page 407

"**listPrincipals** command" on page 387

"**removeSolutions** command" on page 409

"**listSolutions** command" on page 388

Defining a project area by using the command line:

You use project areas to limit the effects of resetting the test environment. You can define new project areas or define a default project area if you did not run the Define Default Project Area task when you configured IBM Case Manager.

Before you begin

Be sure to have your completed configuration checklist available.

About this task

You can assign specific solutions and users to each project area. Each user can belong only to one project area and the default project area. Users can define and modify solutions only in the project area that they are assigned to. Users who are not assigned to a project area cannot log into Case Manager Builder.

When you define a project area, you are prompted to select a connection point for use with the target object store for the new project area. After you define the project area, you have the option to reuse a target object store and its associated connection point when you define another project area. Do not reuse a target object store and connection point.

Procedure

To define a project area:

1. Change the current directory to the *install_path*/CaseManagement/configure directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the /opt/IBM/CaseManagement directory.
Windows	By default, *install_path* is the C:\Program Files\IBM\CaseManagement directory for a fresh install or the C:\Program Files (x86)\IBM\CaseManagement directory for an upgrade.

2. Run the following command. Do not enter any line breaks when you enter the command.

```
configmgr_cl defineProjectArea
 -profile myprofile
 -projectAreaName project_area_name
 -projectAreaDesc project_area_description
 -peConnPt connection_point_name
[-help]
```

-profile *myprofile*
Specifies the development profile that is associated with the project area. The object store and Content Engine properties from the profile are used to create the project area. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-projectAreaName *project_area_name*
The name of the project area. The default project area is named dev_env_connection_definition. The name can contain up to 255 characters. If the name includes a space, put the name in double quotation marks, for example, "Credit Dispute Area". The name cannot contain any of the following characters: \ / : * ? " < > |

-projectAreaDesc *project_area_description*
The description can contain up to 255 characters. If the description includes a space, put the description in double quotation marks, for example, "Solutions for credit card disputes".

-peConnPt *connection_point_name*
The connection point to use with this project area.

-help
Optional and displays a brief message on the command syntax instead of running the command.

What to do next

You can assign users and solutions to the project area.

Related reference:

"**defineProjectArea** command" on page 330

"**deleteProjectArea** command" on page 332

"**modifyProjectArea** command" on page 397

Adding users to a project area by using the command line:

You can add users to a project area or to the default project area. Users cannot log in to Case Manager Builder until they are added to a project area.

Before you begin

Be sure to have your completed configuration checklist available.

About this task

Each user can belong to only one project area and the default project area. If you assigned a user who is already assigned to any nondefault project area to another project area, that user is automatically removed from the original nondefault project area.

You can add groups to the default project area only. You must add users individually to your nondefault project areas.

Procedure

To add users to a project area:

1. Change the current directory to the *install_path*/CaseManagement/configure directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the /opt/IBM/CaseManagement directory.
Windows	By default, *install_path* is the C:\Program Files\IBM\CaseManagement directory for a fresh install or the C:\Program Files (x86)\IBM\CaseManagement directory for an upgrade.

2. Optional: List the users or groups that are already signed to the project area by running the following command. Do not enter any line breaks when you enter the command.

```
configmgr_cl listPrincipals -projectAreaName project_area_name
 -profile myprofile
 [-silent] [-force][-help]
```

-projectAreaName *project_area_name*

The name of the project area. The default project area is named dev_env_connection_definition. The name can contain up to 255 characters. If the name includes a space, put the name in double quotation marks, for example, "Credit Dispute Area". The name cannot contain any of the following characters: \ / : * ? " < > |

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional and displays a brief message on the command syntax instead of running the command.

3. Add a users or groups by running the following command. Do not enter any line breaks when you enter the command.

```
configmgr_cl addPrincipals -projectAreaName project_area_name
 -profile myprofile
 [-users user_name] [-groups group_name]
 [-silent] [-force][-help]
```

-projectAreaName *project_area_name*
Specifies the name of the project area to add users to. The default project area is named dev_env_connection_definition.

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-users *user_name*

Specifies the short name or display name of the user that you want to add. A user can belong to the default project area and one other project area. If you add a user to a nondefault project area, that user is removed from any other nondefault project area.

You can add multiple users at one time by adding additional `-users` *`user_name`* entries on the same command.

You can omit this option if you are adding only groups.

`-groups` ***`group_name`***

Specifies the short name or display name of the group that you want to add. Groups can be added to the default project area only.

You can add multiple groups at one time by adding additional `-groups` *`group_name`* entries on the same command.

You can omit this option if you are adding only users.

`-silent`
Optional: When you specify the **`-silent`** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **`-silent`** parameter, you must also specify the **`-force`** parameter.

`-force`
Optional and applies only when the **`-silent`** parameter is used. When you specify the **`-force`** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

`-help`
Optional and displays a brief message on the command syntax instead of running the command.

4. Repeat the previous step to add more users or groups for the project area.

Related reference:

"**removePrincipals** command" on page 407

"**addPrincipals** command" on page 316

"**listPrincipals** command" on page 387

Adding solutions to a project area by using the command line:

You can add solutions to a project area or to the default project area. A solution can belong to only one project area.

Before you begin

Be sure to have your completed configuration checklist available.

About this task

When a business analyst creates a solution in Case Manager Builder, the solution is added to the project area that the user belongs to. However, you can assign the solution to a different project area. When you assign a solution to a project area, the solution is removed from the project area to which it was previously assigned.

Procedure

To add solutions to a project area:

1. Change the current directory to the *install_path*/CaseManagement/configure directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the /opt/IBM/CaseManagement directory.
Windows	By default, *install_path* is the C:\Program Files\IBM\CaseManagement directory for a fresh install or the C:\Program Files (x86)\IBM\CaseManagement directory for an upgrade.

2. Add one or more solutions by running the following command. Do not enter any line breaks when you enter the command.

```
configmgr_cl addSolutions -projectAreaName project_area_name
 -profile myprofile
 -solutions solution_name [-solutions solution_name_n]
 [-help]
```

-projectAreaName *project_area_name*
Specifies the name of the project area to add solutions to. The default project area is named dev_env_connection_definition.

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-solutions *solution_name*
Specifies the solution name to add to the project area. You can enter multiple -solutions *solution_name* options on the same command line.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

3. Repeat the previous step to add more solutions to the project area.

Related reference:

"**removeSolutions** command" on page 409

"**addSolutions** command" on page 318

Creating a list of object store properties and document types by using the command line

You can reuse existing Content Engine properties and document types in your case management solutions. You can use the command line to create text files that provide the information from a target object store that you need for reusing existing properties and document types.

About this task

When you create the list of properties and document types, the information data is stored in the `PropertyTemplates.csv` and `DocumentTypes.csv` files. These files are comma-separated value text files that you can open in a spreadsheet program or text editor.

The `PropertyTemplates.csv` file contains the following values for the properties in the object store:

- Property Template Display Name
- Symbolic Name
- Data Type
- Description
- Cardinality (single value or multi-value choice list)
- Default Value
- Min Value
- Max Value
- Max Length
- Choice List
- Required
- Hidden

The `DocumentTypes.csv` file contains the following values for the document types in the object store:

- Display Name,
- Symbolic Name
- Descriptive Text
- Is Hidden
- Is Persistent
- Properties (symbolic names of properties associated with this document type)

Procedure

To create a list of the object store properties and document types in an object store:

1. Change the current directory to the *install_path*`/CaseManagement/configure` directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the `/opt/IBM/CaseManagement` directory.

Option	Description
Windows	By default, *install_path* is the `C:\Program Files\IBM\CaseManagement` directory for a fresh install or the `C:\Program Files (x86)\IBM\CaseManagement` directory for an upgrade.

2. Generate the text input file by running the following command. Do not enter any line breaks when you enter the command:

```
configmgr_cl generate_input_sa -operation list
 -file input_file_name
  [-silent] [-force] [-help]
```

-file *input_file_name*

Specifies the full path to the XML input file to create.

Restriction: The directory structure in the path must exist. You can use any valid file name, but the `.txt` extension is recommended. For example, use `-file C:\propertylist\propertylist.txt`.

-silent

Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force

Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help

Optional: Shows a brief message on the command syntax instead of running the command.

For example, the following command creates the `C:\propertylist\propertylist.XML` input file:

```
configmgr_cl generate_input_sa -operation list
 -file "C:\propertylist\propertylist.txt"
```

The *input_file_name* file is created.

3. Edit the property values in the *input_file_name* file.
   a. Open the *input_file_name* file in a text editor.
   b. Provide a value for each property in the file. For example, enter the Content Engine server WSI URL value:

```
CEWS_URI=http://myserver:9080/wsi/FNCEWS40MTOM
```

   c. Save and close the input file.
4. Apply the values in the text input file by running the following command. Do not enter any line breaks when you enter the command:

```
configmgr_cl execute_sa -operation list
 -file "C:\propertylist\propertylist.txt"
```

The two CSV files are created.

5. Provide copies of the CSV files to your business analysts who design solutions in Case Manager Builder. You can open the CSV files in a text editor, a spreadsheet, or other program to review the list of available document types or property templates and their settings.

Related reference:

"**generate_input_sa** command" on page 358

"**execute_sa** command" on page 341

Copying an existing solution by using the command line

You can copy an existing solution to quickly begin designing a new solution that is based on the existing solution. You can use the command line to create the copy.

About this task

You can create a copy of an existing solution in the same object store. You must specify a new name and solution prefix for the new solution because these values must be unique.

You can either reuse the existing properties or document types from the original solution, or you can select the option to create new properties or document types when you deploy the new solution. When you reuse existing properties or document types in a solution, you cannot redefine them in Case Manager Builder. You can remove the property or document type from the solution in Case Manager Builder, but you cannot change any of the attributes, such as data type.

Restriction: You cannot copy a solution that contains locked items.

Procedure

To copy a solution:

1. Change the current directory to the *install_path*/CaseManagement/configure directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the /opt/IBM/CaseManagement directory.
Windows	By default, *install_path* is the C:\Program Files\IBM\CaseManagement directory for a fresh install or the C:\Program Files (x86)\IBM\CaseManagement directory for an upgrade.

2. Generate the text input file by running the following command. Do not type any line breaks when you enter the command:

```
configmgr_cl generate_input_sa -operation copy
 -file input_file_name
[-help]
```

-file *input_file_name*

Specifies the full path to the text input file to create. The directory structure in the path must exist. You can use any valid file name, but the .txt extension is recommended. For example, use -file C:\solutions\copy_input.txt.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

For example, the following command creates the `C:\solutions\copy_input.txt` input file:

```
configmgr_cl generate_input_sa -operation list
 -file C:\solutions\copy_input.txt
```

3. Edit the property values in the *input_file_name* file.
   a. Open the *input_file_name* file in a text editor.
   b. Provide a value for each property in the file. For example, enter the Content Engine server WSI URL value:

      ```
      CEWS_URI=http://myserver:9080/wsi/FNCEWS40MTOM
      ```

   c. Save and close the input file.
4. Apply the values in the text input file by running the following command. Do not type any line breaks when you enter the command:

   ```
   configmgr_cl execute_sa -operation copy
    -file input_file_name
   ```

Related reference:

"**generate_input_sa** command" on page 358

"**execute_sa** command" on page 341

Creating a solution from a template by using the command line

You can create a solution that is based on a solution template to quickly begin designing a new solution. The template provides a basic design for your solution, and you can customize the new solution later in Case Manager Builder. You can use the command line to create the solution. Your administrator determines the templates that are available in an object store.

About this task

If you are a business analyst and want to create a basic solution from a template, you can use Case Manager Builder. However, if you create a solution in Case Manager Builder, you do not have the option to preserve the unique identifiers of any of the objects in the solution.

Creating a solution from a template applies only in the development environment.

Procedure

To create a solution from a template:

1. Change the current directory to the *install_path*`/CaseManagement/configure` directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the `/opt/IBM/CaseManagement` directory.
Windows	By default, *install_path* is the `C:\Program Files\IBM\CaseManagement` directory for a fresh install or the `C:\Program Files (x86)\IBM\CaseManagement` directory for an upgrade.

2. Generate the text input file by running the following command. Do not enter any line breaks when you enter the command:

   ```
   configmgr_cl generate_input_sa -operation createFromTemplate
    -file input_file_name
   [-help]
   ```

   -file *input_file_name*

   Specifies the full path to the text input file to create. The directory structure in the path must exist. You can use any valid file name, but the `.txt` extension is recommended. For example, use `-file C:\solutions\ from_template_input.txt`.

   -help
   Optional: Shows a brief message on the command syntax instead of running the command.

   For example, the following command creates the `C:\solutions\ from_template_input.txt` input file:

   ```
   configmgr_cl generate_input_sa -operation createFromTemplate
    -file C:\solutions\from_template_input.txt
   ```

3. Edit the property values in the *input_file_name* file.
   a. Open the *input_file_name* file in a text editor.
   b. Provide a value for each property in the file. For example, enter the Content Engine server WSI URL value:

      ```
      CEWS_URI=http://myserver:9080/wsi/FNCEWS40MTOM
      ```

      You can specify whether unique identifiers are preserved when solutions are created from the template later on by providing a value for the preserveIdentifier property.

      Important: Ensure that the preserveIdentifier value is set to the same value that is set in the template unless you have a specific business reason to override the template. If you enter `preserveIdentifier=true`, do not deploy more than one solution that is made from this template to the same target object store.
   c. Save and close the input file.
4. Apply the values in the text input file by running the following command. Do not enter any line breaks when you enter the command:

   ```
   configmgr_cl execute_sa -operation createFromTemplate
    -file input_file_name
   ```

Related reference:

"**generate_input_sa** command" on page 358

"**execute_sa** command" on page 341

Converting a solution to a template by using the command line

You can convert a solution to a template by using the command line. You use templates to quickly create new solutions that are based on the same design as the template. The template contains all the solution design information, but you cannot edit a template directly or create running cases from a template.

About this task

Restriction: You cannot convert a solution that contains any locked items.

Procedure

To convert a solution to a template:

1. Change the current directory to the *install_path*/CaseManagement/configure directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the /opt/IBM/CaseManagement directory.
Windows	By default, *install_path* is the C:\Program Files\IBM\CaseManagement directory for a fresh install or the C:\Program Files (x86)\IBM\CaseManagement directory for an upgrade.

2. Generate the text input file by running the following command. Do not enter any line breaks when you enter the command:

```
configmgr_cl generate_input_sa -operation convertToTemplate
 -file input_file_name
  [-help]
```

   -file *input_file_name*

   Specifies the full path to the text input file to create. The directory structure in the path must exist. You can use any valid file name, but the .txt extension is recommended. For example, use -file C:\solutions\to_template_input.txt.

   -help
   Optional: Shows a brief message on the command syntax instead of running the command.

   For example, the following command creates the C:\solutions\to_template_input.txt input file:

```
configmgr_cl generate_input_sa -operation createFromTemplate
 -file C:\solutions\to_template_input.txt
```

3. Edit the property values in the *input_file_name* file.
   a. Open the *input_file_name* file in a text editor.
   b. Provide a value for each property in the file. For example, enter the Content Engine server WSI URL value:

```
CEWS_URI=http://myserver:9080/wsi/FNCEWS40MTOM
```

      You can specify whether unique identifiers are preserved by providing a value for the preserveIdentifier property. The default setting is preserveIdentifier=false.

      Important: For most solutions, do not change the default setting. However, if this solution contains assets that are not managed by Case Manager Builder, such as forms or search templates whose unique identifiers are referenced by non-IBM Case Manager programs, you might want the identifiers to be preserved. If you enter preserveIdentifier=true, do not deploy more than one solution that is made from this template to the same target object store.

   c. Save and close the input file.
4. Apply the values in the text input file by running the following command. Do not type any line breaks when you enter the command:

```
configmgr_cl execute_sa -operation convertToTemplate
 -file input_file_name
```

Related reference:

"**generate_input_sa** command" on page 358

"**execute_sa** command" on page 341

Exporting a solution package by using the command line

You must export the case management solution package from the development environment domain before you can move the solution to the production environment domain. You can use the command line to export the solution package.

Before you begin

Ensure that the solution does not contain locked items. You cannot export a solution that contains locked items.

Be sure to have your completed configuration checklist available.

About this task

A solution package consists of the assets in the solution folder in a case management design object store. The package includes these items:

- The solution definition file.
- The connection definition.
- The task steps (stored as one XPDL file per case type).
- The Pages subfolder.
- The default page objects and any custom page objects that you created in the development environment.
- Any documents, objects, or folders that were in the solution folder at the time of export, including those added by the user.

Procedure

To export the solution package:

1. Change the current directory to the *install_path*/CaseManagement/configure directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the /opt/IBM/CaseManagement directory.
Windows	By default, *install_path* is the C:\Program Files\IBM\CaseManagement directory for a fresh install or the C:\Program Files (x86)\IBM\CaseManagement directory for an upgrade.

2. Run the following command. Do not enter any line breaks when you enter the command.

```
configmgr_cl exportSolution -profile myprofile
 -solutionName solution_name | -solutionTemplateName template_name
 -solutionPackage package_file
 [-help] [-silent] [-force]
```

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-solutionName *solution_name*
Specifies the solution to export. You can omit this option if you are exporting a solution template.

-solutionTemplateName *template_name*
Specifies the solution template to export. You can omit this option if you are exporting a solution.

-solutionPackage *package_file*
Specifies the full path and file name for the exported solution package ZIP file. If the path includes spaces, put the entire path in double quotation marks. For example, enter "C:\Solution Packages\Credit Dispute Solution.zip".

-help
Optional and displays a brief message on the command syntax instead of running the command.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

Results

The solution package ZIP file is created in the folder that you specified.

What to do next

Import the solution package into the new environment.

Related tasks:

"Migrating solutions" on page 131

"Exporting IBM Case Manager assets from a design object store" on page 132

Related reference:

"**exportSolution** command" on page 343

Importing a solution package by using the command line

You must import the case management solution package into the production environment design object store before you can deploy the solution to the production environment domain.

Before you begin

Be sure to have your completed configuration checklist available.

About this task

A solution package consists of the assets in the solution folder in a case management design object store. The package includes these items:

- The solution definition file.
- The connection definition.
- The task steps (stored as one XPDL file per case type).
- The Pages subfolder.
- The default page objects and any custom page objects that you created in the development environment.
- Any documents, objects, or folders that were in the solution folder at the time of export, including those added by the user.

Procedure

To import the solution package:

1. Change the current directory to the *install_path*/CaseManagement/configure directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the /opt/IBM/CaseManagement directory.
Windows	By default, *install_path* is the C:\Program Files\IBM\CaseManagement directory for a fresh install or the C:\Program Files (x86)\IBM\CaseManagement directory for an upgrade.

2. If you need custom service data mapping, create and edit the service data map XML file.
   a. Run the following command. Do not enter any line breaks when you enter the command.

```
configmgr_cl generateServiceDataMap
 -solutionPackage package_file
 -file service_data_map_name
[-help]
```

-solutionPackage *package_file*
Specifies the full path and file name the solution package ZIP file that contains the solution to import. If the path includes spaces, put the entire path in double quotation marks. For example, enter "C:\Solution Packages\Credit Dispute Solution.zip".

-file *service_data_map_name*
Specifies the full path and file name for the service data map XML file to create. The directory structure in the path must already exist. You can use any valid file name, but the .xml extension is recommended. If the path includes a directory name with spaces, enclose the entire path in double quotation marks. For example, enter `"C:\Solution Packages\service_data_map.xml"`.

-help
Optional and displays a brief message on the command syntax instead of running the command.

Tip: You can also use FileNet Deployment Manager to create the service data map file.

b. Use a text editor to edit the values in the service data map XML file. You can change the value for the Name or the URL for the <Destination> elements in the XML file.

3. If you did not use FileNet Deployment Manager to create an object store data map file, run the following command. Do not enter any line breaks when you enter the command.

```
configmgr_cl generateObjectStoreDataMap
 -solutionPackage package_file
 -file object_store_data_map_name
[-help]
```

-solutionPackage *package_file*
Specifies the full path and file name the solution package ZIP file that contains the solution to import. If the path includes spaces, put the entire path in double quotation marks. For example, enter `"C:\Solution Packages\Credit Dispute Solution.zip"`.

-file *object_store_data_map_name*
Specifies the full path and file name for the object store data map XML file to create. The directory structure in the path must already exist. You can use any valid file name, but the .xml extension is recommended. If the path includes a directory name with spaces, enclose the entire path in double quotation marks. For example, enter `"C:\Solution Packages\object_store_data_map.xml"`.

-help
Optional and displays a brief message on the command syntax instead of running the command.

4. Import the solution package by running the following command. Do not enter any line breaks when you enter the command.

```
configmgr_cl importSolution -profile myprofile
 -solutionPackage package_file
 -projectAreaName project_area_name
 -serviceDataMap service_data_map_name
 -objectStoreDataMap object_store_data_map_name
[-silent] [-force]
```

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*`/CaseManagement/configure/profiles` directory. *install_path* is the location where IBM Case Manager is installed.

- The full path to the profile directory, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1"` or `/opt/IBM/CaseManagement/configure/profiles/develop1`.
- The full path to the profile input file, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp"` or `/opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp`.

-solutionPackage *package_file*
Specifies the full path and file name the solution package ZIP file that contains the solution to import. If the path includes spaces, put the entire path in double quotation marks. For example, enter `"C:\Solution Packages\Credit Dispute Solution.zip"`. If you enter a solution name that already exists, the solution will be overwritten in the design object store.

-projectAreaName *project_area_name*
Specifies the name of the project area for the solution. This option is valid only for importing a solution package to into another development environment.

-serviceDataMap *service_data_map_name*
Specifies the full path and file name for the service data map XML file that was generated by using the **generateServiceDataMap** command or by using FileNet Deployment Manager. If the path includes a directory name with spaces, enclose the entire path in double quotation marks. For example, enter `"C:\Solution Packages\service_data_map.xml"`.

If user does not specify a value for -serviceDataMap, the services are mapped to themselves.

-objectStoreDataMap *object_store_data_map_name*
Specifies the full path and file name for the object store data map XML file that was generated by using the **generateObjectStoreDataMap** command or by using FileNet Deployment Manager. If the path includes a directory name with spaces, enclose the entire path in double quotation marks. For example, enter `"C:\Solution Packages\object_store_data_map.xml"`.

If the user does not specify a value for -objectStoreDataMap, the design object store is mapped to the specified profile's design object store. If there is a target object store configured, and a project area is specified, the target object store is mapped to the specified project area's target object store. If there is a target object store and no project area is specified, or if there are other object stores, this value is required.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

Related tasks:

"Distributing solutions as templates" on page 35

Related reference:

"**generateServiceDataMap** command" on page 360

Importing a solution from a manifest by using the command line

You can deploy a case manager solution from a version control system (VCS) into a production environment or a different development environment. You must first extract the solution manifest from the VCS. You then use this manifest to import the solution into the design object store in the new environment before you can deploy the solution to the environment domain.

Before you begin

Run the extract script that you created for the VCS to extract the manifest and related solution files.

Procedure

1. Change the current directory to the *install_path*/CaseManagement/configure directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the /opt/IBM/CaseManagement directory.
Windows	By default, *install_path* is the C:\Program Files\IBM\CaseManagement directory for a fresh install or the C:\Program Files (x86)\IBM\CaseManagement directory for an upgrade.

2. Import the solution manifest by running the following command. Do not enter any line breaks when you enter the command.

```
configmgr_cl importSolutionManifest -profile myprofile
 -solutionManifest mymanifest
 -projectAreaName project_area_name
 [-silent] [-force] [-help]
```

-profile *myprofile*

Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-solutionManifest *mymanifest*

The full path to the solution manifest that you want to import.

If the path includes a directory name with spaces, enclose the path in double quotation marks. For example, enter "C:\Solution Manifests\PREFIX_Manifest.json".

Any files that are related to the solution manifest must be in the same folder as the solution manifest.

Important: Do not rename any of the extracted files including the solution manifest file. Do not modify the content of any of the extracted files.

-projectAreaName *project_area_name*
Specifies the name of the project area for the solution. This option is valid only for importing a solution package to into another development environment.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Generating the object store data map by using the command line

Generate the object store data map for mapping the object stores that are contained in a solution package to the appropriate object stores in the target environment.

About this task

The object store data map XML file is in the same XML format that IBM FileNet Deployment Manager creates and reads. You can change the destination object stores by using a text editor.

Procedure

To generate the object store data map:

1. Change the current directory to the *install_path*/CaseManagement/configure directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the /opt/IBM/CaseManagement directory.
Windows	By default, *install_path* is the C:\Program Files\IBM\CaseManagement directory for a fresh install or the C:\Program Files (x86)\IBM\CaseManagement directory for an upgrade.

2. Generate the object store data map by running the following command. Do not enter any line breaks when you enter the command.

```
configmgr_cl generateObjectStoreDataMap
 -solutionPackage package_file
 -file datamap_file
  [-help]
```

-solutionPackage *package_file*
Specifies the full path and file name of the solution package for which you are creating the data map. If the path includes spaces, put the entire path in double quotation marks. For example, enter `"C:\Solution Packages\Credit Dispute Solution.zip"`.

-file *datamap_file*
Specifies the full path and file name for the data map file to create. The directory structure in the path must already exist. You can use any valid file name, but the .xml extension is recommended. If the path includes a directory name with spaces, put the entire path in double quotation marks. For example, enter `"C:\Solution Packages\datamap.xml"`.

-help
Optional and displays a brief message on the command syntax instead of running the command.

Creating and enabling a Case Analyzer store by using the command line

You must create and enable a Case Analyzer store if you want to use IBM Case Monitor Dashboard. The `createCaseAnalyzerStore` command creates and enables the event export store for the IBM Case Monitor Dashboard.

About this task

You must specify a case management target object store to associate with the Case Analyzer store.

In addition, you must specify the name of the schema to use for the Case Analyzer store. This schema must be present in the database that the Case Analyzer store will use before you create and enable the store.

You can specify a database connection. If you do not specify a database connection, IBM Case Manager uses the database connection for the target object store.

Procedure

To create and enable a Case Analyzer store:

1. Prepare the database for the Case Analyzer store. For more information, see Database administrator installation tasks.
   a. Create JDBC data sources. Run the Configure JDBC Data Sources task by using the IBM FileNet P8 Configuration Manager. For more information, see Editing the Configure JDBC Data Sources tasks and Configuration Manager reference.
   b. Create a database connection. For more information, see Creating a database connection. Based on performance considerations, you might want to share data sources. For more information, see Sharing data sources. You enter the database schema name when you configure and enable the Case Analyzer store by using the IBM Case Manager administration client.
2. Change the current directory to the *install_path*`/CaseManagement/configure` directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the `/opt/IBM/CaseManagement` directory.
Windows	By default, *install_path* is the `C:\Program Files\IBM\CaseManagement` directory for a fresh install or the `C:\Program Files (x86)\IBM\CaseManagement` directory for an upgrade.

3. Create and enable a Case Analyzer store by running the following command. Do not enter any line breaks when you enter the command.

```
configmgr_cl createCaseAnalyzerStore
 -profile myprofile
 -cmtos target_object_store
 -schemaName schema_name
 -dbConnName database_connection
 -eventPruneSchedule pruning_time
 -publishInterval update_interval
 [-silent][-force][-help]
```

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*`/CaseManagement/configure/profiles` directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1"` or `/opt/IBM/CaseManagement/configure/profiles/develop1`.
- The full path to the profile input file, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp"` or `/opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp`.

-cmtos *target_object_store*
Specifies the display name for a case management target object store.

-schemaName *schema_name*
Specifies the name of the schema to use for the Case Analyzer store.

-dbConnName *database_connection*
Specifies the display name of the database connection. You can view and define database connections by using the Administration Console for Content Platform Engine.

-eventPruneSchedule *pruning_time*
Specifies the time each day when unneeded data is to be pruned from the database. Enter the time in the following format: `HH:MM:SS`

If you do not specify a time, pruning is disabled.

-publishInterval *update_interval*
Specifies the interval in minutes when the IBM Case Monitor Dashboard data is to be updated. If you do not specify an interval, the data is updated every 5 minutes.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as

needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Creating and enabling a case history store by using the command line

You must create and enable an event export store if you want to use extended case history features. For example, if you want to view the progression of a case over time by using the Timeline Visualizer widget, you must create and enable a case history store.

Before you begin

You must prepare a database for recording extended case history before you create and enable the case history store.

About this task

You must specify a case management target object store to associate with the case history store. You must also specify the schema name for the case history store database, and a database connection. If a database connection is not specified, the database connection for the target object store is used.

Attention: If the Content Platform Engine server that serves as the backend to the IBM Case Manager system is configured as a cluster, create and enable the case history store when only a single Content Platform Engine server is available. This is typically during a maintenance window when all but one of the application server instances hosting the Content Platform Engine server can be stopped.

Procedure

To create and enable a case history store:

1. Change the current directory to the *install_path*/CaseManagement/configure directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the /opt/IBM/CaseManagement directory.
Windows	By default, *install_path* is the C:\Program Files\IBM\CaseManagement directory for a fresh install or the C:\Program Files (x86)\IBM\CaseManagement directory for an upgrade.

2. Create and enable a case history store by running the following command. Do not enter any line breaks when you enter the command.

```
configmgr_cl createCaseHistoryStore
 -profile myprofile
 -cmtos target_object_store
 -schemaName schema_name
 -dbConnName database_connection
  [-help]
```

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-cmtos *target_object_store*
Specifies the display name for a case management target object store.

-schemaName *schema_name*
Specifies the name of the schema to use for the case history store.

-dbConnName *database_connection*
Specifies the display name of the database connection. You can view and define database connections by using the Administration Console for Content Platform Engine.

-help
Optional and displays a brief message on the command syntax instead of running the command.

Applying a security configuration by using the command line

After you create a security configuration by using the IBM Case Manager administration client, you can apply the security configuration by using the command line. You must specify a target environment if the solution is in a production environment.

Before you begin

The solution must be deployed before you apply the security configuration.

Procedure

To apply a security configuration:

1. Change the current directory to the *install_path*/CaseManagement/configure directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the /opt/IBM/CaseManagement directory.

Option	Description
Windows	By default, *install_path* is the `C:\Program Files\IBM\CaseManagement` directory for a fresh install or the `C:\Program Files (x86)\IBM\CaseManagement` directory for an upgrade.

2. Apply the security configuration by running the following command. Do not enter any line breaks when you enter the command.

```
configmgr_cl applySolutionSecurityManifest
 -profile myprofile
 -targetEnvName target_environment_name
 -solutionName solution_name
 -manifestName manifest_name
  [-help]
```

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*`/CaseManagement/configure/profiles` directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1"` or `/opt/IBM/CaseManagement/configure/profiles/develop1`.
- The full path to the profile input file, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp"` or `/opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp`.

-targetEnvName *target_environment_name*
Specifies the name of the target environment. This argument is required only on production environments.

-solutionName *solution_name*
Specifies the name of the solution that is associated with the security configuration.

-manifestName *manifest_name*
Specifies the name of the security manifest.

-help
Optional and displays a brief message on the command syntax instead of running the command.

Exporting a security configuration by using the command line

You must export the case management security configuration from one domain (such as the testing or development environment) before you can move the security configuration to another domain (such as the production environment). You can use the command line to export one or more security configurations.

About this task

The `exportSolutionSecurityManifest` command exports security configuration settings that are associated with a solution to prepare for importing the security configuration into another IBM Case Manager environment. Security configuration settings are stored in a security manifest file. You must specify a development environment or production environment profile with this command to provide

information about the Content Platform Engine server that contains the security configuration. You can specify the path for the security configuration package or omit the value to use the default name and path.

Procedure

To export the security configuration:

1. Change the current directory to the *install_path*/CaseManagement/configure directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the /opt/IBM/CaseManagement directory.
Windows	By default, *install_path* is the C:\Program Files\IBM\CaseManagement directory for a fresh install or the C:\Program Files (x86)\IBM\CaseManagement directory for an upgrade.

2. Run the following command. Do not enter any line breaks when you enter the command.

```
configmgr_cl exportSolutionSecurityManifest -profile myprofile
 -manifestNames manifest_names -manifestPackage manifest_package_file
 -solutionName solution_name [-silent] [-force] [-help]
```

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-manifestNames *manifest_names*
Specifies the name of the security manifest. To specify more than one manifest at a time, enter multiple -manifestNames options with the command.

-manifestPackage *manifest_package_file*
Specifies the exported security package ZIP file. You can specify the full path and file name for the exported security package ZIP file. If the path includes spaces, put the entire path in double quotation marks. For example, enter "C:\Security Packages\Security1.zip".

If you specify only the file name, the security package is exported to the *ICM_Home*/CaseManagement/configure directory. If you do not specify an option for **-manifestPackage**, the security package is exported to *ICM_Home*/CaseManagement/solution_packages/*SolutionName*_securityManifest.zip.

-solutionName *solution_name*
Specifies the name of the solution that is associated with the security configuration.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Results

The security configuration package ZIP file is created in the folder that you specified.

What to do next

Import the security configuration package into the new environment.

Importing a security configuration by using the command line

If you exported the security configuration package file for a solution when you migrated the solution package, import the file after you deploy the solution in the target environment to apply the security settings to the solution. You can use the command line to import the security configuration package.

Before you begin

The solution that the security configurations are associated with must already be in the design object store.

About this task

You must specify a development environment or production environment profile with this command to provide information about the Content Platform Engine server that you are importing the security configurations to. You can specify the path for the security configuration package or omit the value to use the default name and path.

Procedure

To import the security configuration package:

1. Change the current directory to the *install_path*/CaseManagement/configure directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the `/opt/IBM/CaseManagement` directory.
Windows	By default, *install_path* is the `C:\Program Files\IBM\CaseManagement` directory for a fresh install or the `C:\Program Files (x86)\IBM\CaseManagement` directory for an upgrade.

2. Import the security configuration package by running the following command. Do not enter any line breaks when you enter the command.

```
configmgr_cl importSolutionSecurityManifest -profile myprofile
 -manifestPackage manifest_package_file
 [-silent] [-force] [-help]
```

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*`/CaseManagement/configure/profiles` directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1"` or `/opt/IBM/CaseManagement/configure/profiles/develop1`.
- The full path to the profile input file, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp"` or `/opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp`.

-manifestPackage *manifest_package_file*
Specifies the full path and file name of the security configuration package ZIP file. If the path includes spaces, put the entire path in double quotation marks. For example, enter `"C:\Security Packages\Security1.zip"`.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Applying an audit configuration by using the command line

After you create an audit configuration by using the IBM Case Manager administration client, you can apply the audit configuration by using the command line. You must specify a target environment if the solution is in a production environment.

Before you begin

The solution must be deployed before you apply the audit configuration.

Procedure

To apply an audit configuration:

1. Change the current directory to the *install_path*/CaseManagement/configure directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the /opt/IBM/CaseManagement directory.
Windows	By default, *install_path* is the C:\Program Files\IBM\CaseManagement directory for a fresh install or the C:\Program Files (x86)\IBM\CaseManagement directory for an upgrade.

2. Apply the audit configuration by running the following command. Do not enter any line breaks when you enter the command.

```
configmgr_cl applySolutionAuditManifest
 -profile myprofile
 -targetEnvName target_environment_name
 -solutionName solution_name
 -manifestName manifest_name
  [-help]
```

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-targetEnvName *target_environment_name*
Specifies the name of the target environment. This argument is required only on production environments.

-solutionName *solution_name*
Specifies the name of the solution that is associated with the audit configuration.

-manifestName *manifest_name*
Specifies the name of the audit manifest.

-help
Optional and displays a brief message on the command syntax instead of running the command.

Exporting an audit configuration by using the command line

You must export a case management audit configuration from one domain (such as the testing or development environment) before you can move the audit configuration to another domain (such as the production environment). You can use the command line to export one or more audit configurations.

About this task

The `exportSolutionAuditManifest` command exports audit configuration settings that are associated with a solution to prepare for importing the audit configuration into another IBM Case Manager environment. Audit configuration settings are stored in an audit manifest file. You must specify a development environment or production environment profile with this command to provide information about the Content Platform Engine server that contains the audit configuration. You can specify the path for the audit configuration package or omit the value to use the default name and path.

Procedure

To export the audit configuration:

1. Change the current directory to the *install_path*`/CaseManagement/configure` directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the `/opt/IBM/CaseManagement` directory.
Windows	By default, *install_path* is the `C:\Program Files\IBM\CaseManagement` directory for a fresh install or the `C:\Program Files (x86)\IBM\CaseManagement` directory for an upgrade.

2. Run the following command. Do not enter any line breaks when you enter the command.

```
configmgr_cl exportSolutionAuditManifest -profile myprofile
 - manifestNames manifest_names -manifestPackage manifest_package_file
 - solutionName solution_name [-silent] [-force] [-help]
```

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*`/CaseManagement/configure/profiles` directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1"` or `/opt/IBM/CaseManagement/configure/profiles/develop1`.

- The full path to the profile input file, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp"` or `/opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp`.

-manifestNames ***manifest_names***
Specifies the name of the audit manifest. To specify more than one manifest at a time, enter multiple `-manifestNames` options with the command.

-manifestPackage ***manifest_package_file***
Specifies the exported audit package ZIP file. You can specify the full path and file name for the exported audit package ZIP file. If the path includes spaces, put the entire path in double quotation marks. For example, enter `"C:\Audit Packages\Security1.zip"`.

If you specify only the file name, the audit package is exported to the *ICM_Home*`/CaseManagement/configure` directory. If you do not specify an option for **-manifestPackage**, the audit package is exported to *ICM_Home*`/CaseManagement/solution_packages/`*SolutionName*`_auditManifest.zip`.

-solutionName ***solution_name***
Specifies the name of the solution that is associated with the audit configuration.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Results

The audit configuration package ZIP file is created in the folder that you specified.

What to do next

Import the audit configuration package into the new environment.

Importing an audit configuration by using the command line

If you exported the audit configuration package file for a solution when you migrated the solution package, import the file after you deploy the solution in the target environment to apply the audit settings to the solution. You can use the command line to import the audit configuration package.

Before you begin

The solution that the audit configurations are associated with must already be in the design object store.

About this task

You must specify a development environment or production environment profile with this command to provide information about the Content Platform Engine server that you are importing the audit configurations to. You can specify the path for the audit configuration package or omit the value to use the default name and path.

Procedure

To import the audit configuration package:

1. Change the current directory to the *install_path*/CaseManagement/configure directory. *install_path* is the location where IBM Case Manager is installed.

Option	Description
AIX Linux	By default, *install_path* is the /opt/IBM/CaseManagement directory.
Windows	By default, *install_path* is the C:\Program Files\IBM\CaseManagement directory for a fresh install or the C:\Program Files (x86)\IBM\CaseManagement directory for an upgrade.

2. Import the audit configuration package by running the following command. Do not enter any line breaks when you enter the command.

```
configmgr_cl importSolutionAuditManifest -profile myprofile
 -manifestPackage manifest_package_file
 [-silent] [-force] [-help]
```

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-manifestPackage *manifest_package_file*
Specifies the full path and file name of the audit configuration package ZIP file. If the path includes spaces, put the entire path in double quotation marks. For example, enter "C:\Audit Packages\Audit1.zip".

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written

to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Command syntax

Syntax diagrams describe how you must enter commands and what options are available.

The syntax topics uses several conventions to indicate variable, parameters, required items, and optional items. Enter all commands on a single line, even if the command or syntax examples wrap to the next line.

```
command_name -option_1 variable_1 [-option_2 variable_2]
 [-option_3 variable_3 | -option_4]
```

Where:

command_name
The **command_name** is required.

-option_1
The **-option_1** parameter is a required parameter.

variable_1
The *variable_1* value is a required variable for the **-option_1** parameter.

[-option_2 *variable_2***]**
Square braces [] indicate optional items. The **-option_2** parameter with its value is optional.

[-option_3 *variable_3* **| -option_4]**
A vertical bar indicates a choice of parameters. Use the **-option_3** parameter with its value, or use the **-option_4** parameter. In this example, both items are optional, and you can use only one or the other.

"**addPrincipals** command" on page 316

"**addSolutions** command" on page 318

"**applySolutionAuditManifest** command" on page 319

"**applySolutionSecurityManifest** command" on page 320

"**checkStatus** command" on page 321

"**createCaseAnalyzerStore** command" on page 328

"**createCaseHistoryStore** command" on page 329

"**defineProjectArea** command" on page 330

"**deleteProjectArea** command" on page 332

"**execute** command" on page 333

"**execute_sa** command" on page 341

addPrincipals command

The **addPrincipals** command adds a user or group to a project area. Users who are not assigned to a project area cannot log in to Case Manager Builder.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl addPrincipals -projectAreaName project_area_name
 -profile myprofile
 [-users user_name] [-groups group_name]
 [-silent] [-force] [-help]
```

Parameters

-projectAreaName *project_area_name*
The name of the project area. The default project area is named `dev_env_connection_definition`. The name can contain up to 255 characters. If the name includes a space, put the name in double quotation marks, for example, `"Credit Dispute Area"`. The name cannot contain any of the following characters: `\ / : * ? " < > |`

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-users *user_name*

Specifies the short name or display name of the user that you want to add. A user can belong to the default project area and one other project area. If you add a user to a nondefault project area, that user is removed from any other nondefault project area.

You can add multiple users at one time by adding additional -users *user_name* entries on the same command.

You can omit this option if you are adding only groups.

-groups *group_name*

Specifies the short name or display name of the group that you want to add. You can add groups only to the default project area.

You can add multiple groups at one time by adding additional -groups *group_name* entries on the same command.

You can omit this option if you are adding only users.

-silent

Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force

Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help

Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Add a single user to a project area.

The following command adds the user MariaG to the project area MyProjectArea in the MyDevelop1 profile:

```
configmgr_cl addPrincipals -projectAreaName MyProjectArea
 -profile MyDevelop1
 -users MariaG
```

Add a single group to the default project area.

The following command adds the group CaseDevelopers to the default project area in the MyDevelop1 profile:

```
configmgr_cl addPrincipals -projectAreaName dev_env_connection_definition
 -profile MyDevelop1
 -groups CaseDevelopers
```

Add several users to a project area.

The following command adds the users MariaG, BarneyF, and JoseP to the project area MyProjectArea in the MyDevelop1 profile:

```
configmgr_cl addPrincipals -projectAreaName MyProjectArea
 -profile MyDevelop1
 -users MariaG -users BarneyF -users JoseP
```

Add several users and a single group to the default project area.

The following command adds the users MariaG, BarneyF, and JoseP and the group CaseDevelopers to the default project area in the MyDevelop1 profile:

```
configmgr_cl addPrincipals -projectAreaName dev_env_connection_definition
 -profile MyDevelop1
 -users MariaG -users BarneyF -users JoseP
 -groups CaseDevelopers
```

Show the help for the addPrincipals command.

The following command shows the help for the **addPrincipals** command:

```
configmgr_cl addPrincipals -help
```

Related reference:

"**removePrincipals** command" on page 407

"**listPrincipals** command" on page 387

addSolutions command

The **addSolutions** command adds a solution to a project area. A solution can belong to only one project area.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl addSolutions -projectAreaName project_area_name
 -profile myprofile
 -solutions solution_name [-solutions solution_name_n]
 [-silent] [-force] [-help]
```

Parameters

-projectAreaName *project_area_name*

Specifies the name of the project area to add the solution to. The default project area is named dev_env_connection_definition.

-profile *myprofile*

Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.

- The full path to the profile input file, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp"` or `/opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp`.

-solutions *solution_name*
Specifies the solution name to add to the project area. You can enter multiple `-solutions` *solution_name* options on the same command line.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Add a solution to the project area.
The following command adds the Solution1 solution to the project area CreditDisputeArea for the development environment that was configured with the myDevelop1 profile:

```
configmgr_cl addSolutions -projectAreaName CreditDisputeArea
 -profile myDevelop1
 -solutions Solution1
 [-silent] [-force]
```

Add two solutions to the project area.
The following command adds the Solution1 solution and the Solution2 solution to the project area CreditDisputeArea for the development environment that was configured with the myDevelop1 profile:

```
configmgr_cl addSolutions -projectAreaName CreditDisputeArea
 -profile myDevelop1
 -solutions Solution1 -solutions Solution2
 [-silent] [-force]
```

Show the help for the addSolutions command.
The following command shows the help for the **addSolutions** command:

```
configmgr_cl addSolutions -help
```

Related reference:

"**removeSolutions** command" on page 409

applySolutionAuditManifest command

The **applySolutionAuditManifest** command applies a solution audit configuration that you previously created by using the IBM Case Manager administration client. The solution must be deployed before you apply the audit configuration. You must specify a target environment if the solution is in a production environment.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl applySolutionAuditManifest
 -profile myprofile
 -targetEnvName target_environment_name
 -solutionName solution_name
 -manifestName manifest_name
  [-silent][-force][-help]
```

Parameters

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-targetEnvName *target_environment_name*
Specifies the name of the target environment. This argument is required only on production environments.

-solutionName *solution_name*
Specifies the name of the solution that is associated with the audit configuration.

-manifestName *manifest_name*
Specifies the name of the audit manifest.

-help
Optional and displays a brief message on the command syntax instead of running the command.

applySolutionSecurityManifest command

The **applySolutionSecurityManifest** command applies a solution security configuration that you have previously created by using the IBM Case Manager administration client. The solution must be deployed before you apply the security configuration. You must specify a target environment if the solution is in a production environment.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl applySolutionSecurityManifest
 -profile myprofile
 -targetEnvName target_environment_name
 -solutionName solution_name
 -manifestName manifest_name
  [-silent][-force][-help]
```

Parameters

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-targetEnvName *target_environment_name*
Specifies the name of the target environment. This argument is required only on production environments.

-solutionName *solution_name*
Specifies the name of the solution that is associated with the security configuration.

-manifestName *manifest_name*
Specifies the name of the security manifest.

-help
Optional and displays a brief message on the command syntax instead of running the command.

checkStatus command

The **checkStatus** command checks the status of the specified configuration task.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl checkStatus [-task task_type | -taskfile task_file_name]
 -profile myprofile [-help]
```

Parameters

-task *task_type*
Specifies which task to use for the status check. You can omit the **-task** *task_type* parameter if you want to check all of the tasks or if you specify the **-taskfile** *task_file_name* parameter. The following table lists the valid task names, the associated configuration XML file, and a description of the settings affected by the task.

Table 31. task_type values

Option	Configuration file	Description
No value specified.	A WebSphere Application Server development environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configibmbpm.xml` • `configibmcm.xml` • `configrules.xml` • `createapps.xml` • `definedefaultprojectarea.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deploycmbapp.xml` • `deployibmbpmis.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registercpeapplets.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerprojectarea.xml` • `registerservices.xml` • `updatecpeclient.xml`	Checks the status of all tasks. If you omit the `-task` *`task_type`* parameter and the **`-taskfile`** *task_file_name* parameter, the status for all the configuration files in the profile is shown.
No value specified.	An Oracle WebLogic Server development environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configrules.xml` • `createapps.xml` • `definedefaultprojectarea.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deploycmbapp.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registercpeapplets.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerprojectarea.xml` • `registerservices.xml` • `updatecpeclient.xml`	Checks the status of all tasks. If you omit the `-task` *`task_type`* parameter and the **`-taskfile`** *task_file_name* parameter, the status for all the configuration files in the profile is shown.

Table 31. task_type values (continued)

Option	Configuration file	Description
No value specified.	A WebSphere Application Server production environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configibmbpm.xml` • `configibmcm.xml` • `configrules.xml` • `createapps.xml` • `definetargetenv.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deployibmbpmis.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `deploysolution.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registercpeapplets.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerservices.xml` • `registertargetenv.xml` • `updatecpeclient.xml`	Checks the status of all tasks. If you omit the `-task` *`task_type`* parameter and the **`-taskfile`** *task_file_name* parameter, the status for all the configuration files in the profile is shown.
No value specified.	An Oracle WebLogic Server production environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configrules.xml` • `createapps.xml` • `definetargetenv.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `deploysolution.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerservices.xml` • `registertargetenv.xml` • `updatecpeclient.xml`	Checks the status of all tasks. If you omit the `-task` *`task_type`* parameter and the **`-taskfile`** *task_file_name* parameter, the status for all the configuration files in the profile is shown.

Table 31. task_type values (continued)

Option	Configuration file	Description
`configcaseloginmodules`	`configcaseloginmodules.xml`	Checks the status of the task for configuring the login modules for the Case Manager Builder application. The login modules provide authentication information for the Case Manager Builder application. If you are deploying Case Manager Builder to the same application server where Content Engine is deployed, skip this task.
`configcmos`	`configcmos.xml`	Checks the status for configuring the object stores. This task installs the IBM Case Manager Add-ons and creates the required events and subscriptions in Content Engine.
`configibmbpm`	`configibmbpm.xml`	Checks the status of configuring IBM Business Process Manager task. This task configures the connection to the IBM Business Process Manager host server. This task is required if you use IBM Business Process Manager as the workflow server for IBM Case Manager.
`configibmcm`	`configibmcm.xml`	Checks the status for configuring IBM Content Manager Host
`configrules`	`configrules.xml`	Checks the status of the task that configures business rules in your solution.

Table 31. task_type values (continued)

Option	Configuration file	Description
`configureldap`	`configureldap.xml` `configureldap.`*n*`.xml` . *n* is an integer starting with 2.	Checks the status for configuring the directory service provider (LDAP) settings for the Case Manager Builder application. The directory service provider (LDAP) settings define the directory service and the users and groups that uses for authentication. If you have one or more `configureldap.`*n*`.xml` files in a profile, you must use the **`-taskfile`** *task_file_name* option to run a single task file.
`createapps`	`createapps.xml`	Checks the status for the task that updates the IBM Case Manager API WAR file and the Case Manager Builder EAR file with system parameters.
`definedefaultprojectarea`	`definedefaultprojectarea.xml`	Checks the status for defining the default project area for the development environment.
`definetargetenv`	`definetargetenv.xml`	Checks the status for the task that defines a target environment for the production environment.
`deploycaseapi`	`deploycaseapi.xml`	Checks the status of the task for deploying the IBM Case Manager API application on the web application server. Deploying the IBM Case Manager API application makes the application available for use by theIBM Case Manager application.

Table 31. task_type values (continued)

Option	Configuration file	Description
`deploycaseforms`	`deploycaseforms.xml`	Checks the status for deploying forms applications.
`deploycmbapp`	`deploycmbapp.xml`	Checks the status for deploying a Case Manager Builder instance on the web application server. Deploying makes the Case Manager Builder application available for use.
`deployibmbpmis`	`deployibmbpmis.xml`	Checks the status for the task that deploys the IBM Business Process Manager integration service.
`deployregisterwidgets`	`deployregisterwidgets.xml`	Checks the status for the task that registers and deploys a widget package with Case Manager Builder and IBM Content Navigator.
`deploysolution`	`deploysolution.xml` `deploysolution.`*n*`.xml`. *n* is an integer starting with 2.	Checks the status for deploying an IBM Case Manager solution into a production target object store. You need one configuration file for each production environment target object store that you deploy a solution to. When you generate a second solution deployment configuration file in a profile, it is named `deploysolution.2.xml`. The file name increments for each new file that you generate. You cannot change the file name, but you can edit the value in the file for the name of the task.

Table 31. task_type values (continued)

Option	Configuration file	Description
registeradmin	registeradmin.xml	Checks the status for the task that registers the IBM Case Manager administration client with IBM Content Navigator.
registerexternaldataurl	registerexternaldataurl.xml	Checks the status for the task that registers a data source other than Content Platform Engine.
registerprojectarea	registerprojectarea.xml	Checks the status for the task that registers the project area with IBM Content Navigator and configures the Content Platform Engine repositories.
registertargetenv	registertargetenv.xml	Checks the status for the task that registers the target environment with IBM Content Navigator and configures the Content Platform Engine repositories.
registerexternaldataurl	registerexternaldataurl.xml	Checks the status for registering an external data source URL.
updatecpeclient	updatecpeclient.xml	Checks the status for the task that updates the client connector files for Content Platform Engine.

-taskfile *task_file_name*
Specifies the *configuration*.xml file to use.

If only one task file exists for the *task_type*, the **-taskfile** *task_file_name* parameter is optional.

If more than one task file for the *task_type* exists, you must include the **-taskfile** *task_file_name* parameter. The *task_file* value is case sensitive if your operating system is case sensitive for file names.

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.

- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Check the status for configuring the login modules for the development environment.

The following command checks the status of the configcaseloginmodules task in the *install_path*/CaseManagement/configure/profiles/develop1 directory:

```
configmgr_cl checkStatus -task configcaseloginmodules
-profile develop1
```

Show the help for the checkStatus command.

The following command shows the help for the **checkStatus** command:

```
configmgr_cl checkStatus -help
```

createCaseAnalyzerStore command

The **createCaseAnalyzerStore** command creates and enables a Case Analyzer store for use with the IBM Case Monitor Dashboard.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl createCaseAnalyzerStore
 -profile myprofile
 -cmtos target_object_store
 -schemaName schema_name
 -dbConnName database_connection
 -eventPruneSchedule pruning_time
 -publishInterval update_interval
 [-silent][-force][-help]
```

Parameters

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-cmtos *target_object_store*
Specifies the display name for a case management target object store.

-schemaName *schema_name*
Specifies the name of the schema to use for the Case Analyzer store.

-dbConnName *database_connection*
Specifies the display name of the database connection. You can view and define database connections by using the Administration Console for Content Platform Engine.

-eventPruneSchedule *pruning_time*
Specifies the time each day when unneeded data is to be pruned from the database. Enter the time in the following format: `HH:MM:SS`

If you do not specify a time, pruning is disabled.

-publishInterval *update_interval*
Specifies the interval in minutes when the IBM Case Monitor Dashboard data is to be updated. If you do not specify an interval, the data is updated every 5 minutes.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

createCaseHistoryStore command

The **createCaseHistoryStore** command creates and enables an event case history for use with extended case history features. For example, if you want to view the progression of a case over time by using the Timeline Visualizer widget, you must create and enable a case history store.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl createCaseHistoryStore
 -profile myprofile
 -cmtos target_object_store
 -schemaName schema_name
 -dbConnName database_connection
  [-silent][-force][-help]
```

Parameters

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-cmtos *target_object_store*
Specifies the display name for a case management target object store.

-schemaName *schema_name*
Specifies the name of the schema to use for the case history store.

-dbConnName *database_connection*
Specifies the display name of the database connection. You can view and define database connections by using the Administration Console for Content Platform Engine.

-help
Optional and displays a brief message on the command syntax instead of running the command.

defineProjectArea command

The **defineProjectArea** command defines a new project area for the development environment. You use project areas to limit the effects of resetting the test environment. You can define new project areas or define a default project area if you did not run the Define Default Project Area task when you configured IBM Case Manager.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl defineProjectArea
 -profile myprofile
 -projectAreaName project_area_name
 -projectAreaDesc project_area_description
 -peConnPt connection_point_name
  [-silent] [-force] [-help]
```

Parameters

-profile *myprofile*
Specifies the development profile that is associated with the project area. The object store and Content Engine properties from the profile are used to create the project area. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-projectAreaName *project_area_name*
The name of the project area. The default project area is named `dev_env_connection_definition`. The name can contain up to 255 characters. If the name includes a space, put the name in double quotation marks, for example, `"Credit Dispute Area"`. The name cannot contain any of the following characters: `\ / : * ? " < > |`

-projectAreaDesc *project_area_description*
The description can contain up to 255 characters. If the description includes a space, put the description in double quotation marks, for example, `"Solutions for credit card disputes"`.

-peConnPt *connection_point_name*
The connection point to use with this project area.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Define the default project area.
The following command defines the default project area for the development environment that was configured with the myDevelop1 profile:

```
configmgr_cl defineProjectArea
 -profile myDevelop1
 -projectAreaName dev_env_connection_definition
 -projectAreaDesc "Default project area for myDevelop1"
 -peConnPt connpoint1
  [-silent] [-force]
```

Define a new project area.
The following command defines the new project area CreditDisputeArea for the development environment that was configured with the myDevelop1 profile:

```
configmgr_cl defineProjectArea
 -profile myDevelop1
 -projectAreaName CreditDisputeArea
 -projectAreaDesc "Credit card dispute project area for myDevelop1"
 -peConnPt connpoint1
  [-silent] [-force]
```

Show the help for the defineProjectArea command.

The following command shows the help for the **defineProjectArea** command:

```
configmgr_cl defineProjectArea -help
```

Related reference:

"**deleteProjectArea** command"

"**modifyProjectArea** command" on page 397

deleteProjectArea command

The **deleteProjectArea** command deletes a project area from the development environment. You cannot delete the default project area or a project area that has solutions assigned to it.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl deleteProjectArea
 -profile myprofile
 -projectAreaName project_area_name
 [-silent] [-force] [-help]
```

Parameters

-profile *myprofile*

Specifies the development profile that is associated with the project area. The object store and Content Engine properties from the profile are used to create the project area. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-projectAreaName *project_area_name*

The name of the project area. The default project area is named dev_env_connection_definition. The name can contain up to 255 characters. If the name includes a space, put the name in double quotation marks, for example, "Credit Dispute Area". The name cannot contain any of the following characters: \ / : * ? " < > |

-silent

Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force

Optional and applies only when the **-silent** parameter is used. When you

specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Delete a project area.
The following command deletes the CreditDisputeArea project area from the development environment that was configured with the myDevelop1 profile:

```
configmgr_cl deleteProjectArea
 -profile Develop1
 -projectAreaName CreditDisputeArea
 [-silent] [-force]
```

Show the help for the deleteProjectArea command.
The following command shows the help for the **deleteProjectArea** command:

```
configmgr_cl deleteProjectArea -help
```

Related reference:

"**defineProjectArea** command" on page 330

execute command

The **execute** command applies the settings from a configuration XML file for the specified configuration task.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl execute [-task task_type | -taskfile task_file_name]
 -profile myprofile [-silent] [-force] [-help]
```

Parameters

-task *task_type*
Indicates which task to run. You can omit the **-task** *task_type* parameter if you want to run all of the tasks or if you specify the **-taskfile** *task_file_name* parameter. The following table describes the valid task names, the associated configuration XML file, and a description of the settings affected by the task.

Table 32. task_type values

Option	Configuration file	Description
No value is specified.	A WebSphere Application Server development environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configibmbpm.xml` • `configibmcm.xml` • `configrules.xml` • `createapps.xml` • `definedefaultprojectarea.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deploycmbapp.xml` • `deployibmbpmis.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registercpeapplets.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerprojectarea.xml` • `registerservices.xml` • `updatecpeclient.xml`	Runs all the tasks in the profile. If you omit the `-task` *`task_type`* parameter and the **`-taskfile`** *task_file_name* parameter, the tool runs all of the configuration files in the profile. Any configuration XML file that has the enabled attribute value in the <configuration> element set to false is skipped.

Table 32. task_type values (continued)

Option	Configuration file	Description
No value is specified.	A WebSphere Application Server development environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configibmbpm.xml` • `configibmcm.xml` • `configrules.xml` • `createapps.xml` • `definedefaultprojectarea.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deploycmbapp.xml` • `deployibmbpmis.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registercpeapplets.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerprojectarea.xml` • `registerservices.xml` • `updatecpeclient.xml`	Runs all the tasks in the profile. If you omit the `-task` *`task_type`* parameter and the **`-taskfile`** *task_file_name* parameter, the tool runs all of the configuration files in the profile. Any configuration XML file that has the enabled attribute value in the <configuration> element set to false is skipped.
No value is specified.	An Oracle WebLogic Server development environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configrules.xml` • `createapps.xml` • `definedefaultprojectarea.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deploycmbapp.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registercpeapplets.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerprojectarea.xml` • `registerservices.xml` • `updatecpeclient.xml`	Runs all the tasks in the profile. If you omit the `-task` *`task_type`* parameter and the **`-taskfile`** *task_file_name* parameter, the tool runs all of the configuration files in the profile. Any configuration XML file that has the enabled attribute value in the <configuration> element set to false is skipped.

Table 32. task_type values (continued)

Option	Configuration file	Description
No value is specified.	A WebSphere Application Server production environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configibmbpm.xml` • `configibmcm.xml` • `configrules.xml` • `createapps.xml` • `definetargetenv.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deployibmbpmis.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `deploysolution.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registercpeapplets.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerservices.xml` • `registertargetenv.xml` • `updatecpeclient.xml`	Runs all the tasks in the profile. If you omit the `-task` *`task_type`* parameter and the **`-taskfile`** *task_file_name* parameter, the tool runs all of the configuration files in the profile. Any configuration XML file that has the enabled attribute value in the <configuration> element set to false is skipped.
No value is specified.	An Oracle WebLogic Server production environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configrules.xml` • `createapps.xml` • `definetargetenv.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `deploysolution.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerservices.xml` • `registertargetenv.xml` • `updatecpeclient.xml`	Runs all the tasks in the profile. If you omit the `-task` *`task_type`* parameter and the **`-taskfile`** *task_file_name* parameter, the tool runs all of the configuration files in the profile. Any configuration XML file that has the enabled attribute value in the <configuration> element set to false is skipped.

Table 32. task_type values (continued)

Option	Configuration file	Description
`configcaseloginmodules`	`configcaseloginmodules.xml`	Runs the task for configuring the login modules for the Case Manager Builder application. The login modules provide authentication information for the Case Manager Builder application. If you are deploying Case Manager Builder to the same application server where Content Platform Engine is deployed, skip this option.
`configcmos`	`configcmos.xml`	Runs the task for configuring the design and target object stores. This task installs the IBM Case Manager Add-ons and creates the required events and subscriptions in Content Platform Engine.
`configibmbpm`	`configibmbpm.xml`	Runs the task that configures the connection to the IBM Business Process Manager host server. This task is required if you use IBM Business Process Manager as the workflow server for IBM Case Manager.
`configibmcm`	`configibmcm.xml`	Runs the task for configuring IBM Content Manager.
`configrules`	`configrules.xml`	Lists the task that configures business rules in your solution.

Table 32. task_type values (continued)

Option	Configuration file	Description
`configureldap`	`configureldap.xml` `configureldap.`*n*`.xml` . *n* is an integer starting with 2.	Runs the task to configure the directory service provider (LDAP) settings. The directory service provider (LDAP) settings define the directory service and the users and groups that IBM Case Manager uses for authentication. If you have one or more `configureldap.`*n*`.xml` files in a profile, you must use the **`-taskfile`** *task_file_name* option to run a single task file.
`createapps`	`createapps.xml`	Lists the task that updates the IBM Case Manager API WAR file and the Case Manager Builder EAR file with system parameters.
`definedefaultprojectarea`	`definedefaultprojectarea.xml`	Checks the status for defining the default project area for the development environment.
`definetargetenv`	`definetargetenv.xml`	Lists the task that defines a target environment for the production environment.
`deploycaseapi`	`deploycaseapi.xml`	Runs the task to deploy the IBM Case Manager API application on the web application server. Deploying the IBM Case Manager API application makes the application available for use by the Case Manager Builder or Case Manager Client application.
`deploycaseforms`	`deploycaseforms.xml`	Runs the task to deploy the forms application.

Table 32. task_type values (continued)

Option	Configuration file	Description
`deploycmbapp`	`deploycmbapp.xml`	Runs the task to deploy a Case Manager Builder instance on the web application server. Deploying makes the Case Manager Builder application available for use.
`deployibmbpmis`	`deployibmbpmis.xml`	Runs the task that deploys the IBM Business Process Manager integration service.
`deployregisterwidgets`	`deployregisterwidgets.xml`	Runs the task that registers and deploys a widget package with Case Manager Builder and IBM Content Navigator.
`deploysolution`	`deploysolution.xml` `deploysolution.`*n*`.xml`. *n* is an integer starting with 2.	Runs the task to deploy a IBM Case Manager solution into a production target object store. If you have one or more `deploysolution.`*n*`.xml` files in a profile, you must use the **`-taskfile`** *task_file_name* option to run a single task file.
`registeradmin`	`registeradmin.xml`	Runs the task that registers the IBM Case Manager administration client with IBM Content Navigator.
`registerexternaldataurl`	`registerexternaldataurl.xml`	Runs the task that registers a data source other than Content Platform Engine.
`registerprojectarea`	`registerprojectarea.xml`	Runs the task that registers the project area with IBM Content Navigator and configures the Content Platform Engine repositories.

Table 32. task_type values (continued)

Option	Configuration file	Description
`registertargetenv`	`registertargetenv.xml`	Runs the task that registers the target environment with IBM Content Navigator and configures the Content Platform Engine repositories.
`registerexternaldataurl`	`registerexternaldataurl.xml`	Runs the task to register an external data source URL.
`updatecpeclient`	`updatecpeclient.xml`	Checks the status for the task that updates the client connector files for Content Platform Engine.

-taskfile *task_file_name*
Specifies the *configuration*`.xml file` to use.

If only one task file exists for the *task_type*, the **-taskfile** *task_file_name* parameter is optional.

If more than one task file for the *task_type* exists, you must include the **-taskfile** *task_file_name* parameter. The *task_file* value is case sensitive if your operating system is case sensitive for file names.

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*`/CaseManagement/configure/profiles` directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1"` or `/opt/IBM/CaseManagement/configure/profiles/develop1`.
- The full path to the profile input file, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp"` or `/opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp`.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Run all the tasks in a profile.
The following command runs all the tasks in the build profile, which is in the *install_path*/CaseManager/configure/profiles/develop1 directory.

```
configmgr_cl execute -profile develop1
```

Run only the configureldap task in a profile that has only one configureldap task.
The following command runs the configureldap.xml file in the build profile, which is in the *install_path*/CaseManager/configure/profiles/develop1 directory:

```
configmgr_cl execute -task configureldap -profile develop1
```

Run only the configureldap.3.xml task file in a profile that has multiple configureldap tasks.
The following command runs the configureldap.3.xml file in the build profile, which is in the *install_path*/CaseManager/configure/profiles/develop3 directory:

```
configmgr_cl execute -taskfile configureldap.3.xml -profile develop3
```

Show the help for the execute command.
The following command shows the help for the **execute** command:

```
configmgr_cl execute -help
```

execute_sa command

The **execute_sa** command applies the values in the input file to copy a solution, create a solution from a template, convert a solution to a template, or list the properties and document types in an object store.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl execute_sa -operation operation_type
 -file input_file_name
 [-silent] [-force] [-help]
```

Parameters

-operation *operation_type*
Indicates the operation to run.

Table 33. Valid operation_type values

Option	Description
copy	Copies a solution.
createFromTemplate	Creates a solution from a template.
list	Creates the CSV files with the properties and document types in an object store.
convertToTemplate	Converts a solution to a template.

-file *input_file_name*

Specifies the full path to the input file that you created with the **generate_input_sa** command. The input file provides Content Engine authentication information and other information for the selected operation. You must edit the property values in the input file before you run the **execute_sa** command.

For example, use `C:\propertylist\propertylist.txt`.

-silent

Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force

Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help

Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Create a list of properties and document types.

The following command creates a list of properties and document types by using the `C:\propertylist` input file:

```
configmgr_cl execute_sa -operation list
 -file C:\propertylist\propertylist.txt
```

Copy an existing solution.

The following command copies a solution by using the values in the `C:\solutions\copy_solution_input.txt` input file:

```
configmgr_cl execute_sa -operation copy
 -file C:\solutions\copy_solution_input.txt
```

Create a solution from a template.

The following command creates a solution from a template by using the values in the `C:\solutions\copy_solution_input.txt` input file:

```
configmgr_cl execute_sa -operation createFromTemplate
 -file C:\solutions\from_template_input.txt
```

Convert a solution to a template.

The following command converts a solution to a template by using the values in the `C:\solutions\copy_solution_input.txt` input file:

```
configmgr_cl execute_sa -operation convertToTemplate
 -file C:\solutions\to_template_input.txt
```

Show the help for the execute_sa command.

The following command shows the help for the **execute_sa** command:

```
configmgr_cl execute_sa -help
```

Related reference:

"**generate_input_sa** command" on page 358

exportSolution command

The **exportSolution** command exports a case management solution or solution template from the development environment domain before you move the solution to another environment.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl exportSolution -profile myprofile
 -solutionName solution_name | -solutionTemplateName template_name
 -solutionPackage package_file
 [-silent] [-force] [-help]
```

Parameters

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-solutionName *solution_name*
Specifies the solution to export. You can omit this option if you are exporting a solution template.

-solutionTemplateName *template_name*
Specifies the solution template to export. You can omit this option if you are exporting a solution.

-solutionPackage *package_file*
Specifies the full path and file name for the exported solution package ZIP file. If the path includes spaces, put the entire path in double quotation marks. For example, enter "C:\Solution Packages\Credit Dispute Solution.zip".

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Export a solution package.
The following command exports the Solution1 solution in the MyDevelop1 profile to the `Solution1.zip` file:

```
configmgr_cl exportSolution -profile myDevelop1
 -solutionName Solution1
 -solutionPackage
"C:\Program Files (x86)\IBM\CaseManagement\solution_packages\Solution1.zip"
```

Export a solution template package.
The following command exports the Template1 solution template in the MyDevelop1 profile to the `Template1.zip` file:

```
configmgr_cl exportSolution -profile myDevelop1
 -solutionTemplateName Template1
 -solutionPackage
"C:\Program Files (x86)\IBM\CaseManagement\solution_packages\Template1.zip"
```

Show the help for the exportSolution command.
The following command shows the help for the **exportSolution** command:

```
configmgr_cl exportSolution -help
```

exportSolutionAuditManifest command

The **exportSolutionAuditManifest** command exports a case management audit configuration from the development environment domain before you move the audit configuration to another environment.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl exportSolutionAuditManifest -profile myprofile
 - manifestNames manifest_names -manifestPackage manifest_package_file
 - solutionName solution_name [-silent] [-force] [-help]
```

Parameters

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*`/CaseManagement/configure/profiles` directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1"` or `/opt/IBM/CaseManagement/configure/profiles/develop1`.
- The full path to the profile input file, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp"` or `/opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp`.

-manifestNames *manifest_names*
Specifies the name of the audit manifest. To specify more than one manifest at a time, enter multiple `-manifestNames` options with the command.

-manifestPackage *manifest_package_file*
Specifies the exported audit package ZIP file. You can specify the full path and file name for the exported audit package ZIP file. If the path includes spaces, put the entire path in double quotation marks. For example, enter `"C:\Audit Packages\Security1.zip"`.

If you specify only the file name, the audit package is exported to the *ICM_Home*`/CaseManagement/configure` directory. If you do not specify an option for **-manifestPackage**, the audit package is exported to *ICM_Home*`/CaseManagement/solution_packages/`*SolutionName*`_auditManifest.zip`.

-solutionName *solution_name*
Specifies the name of the solution that is associated with the audit configuration.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Export a solution audit configuration.
The following command exports the Audit1 audit configuration in the MyDevelop1 profile to the `Audit1.zip` file:

```
configmgr_cl exportSolutionAuditManifest -profile myDevelop1
 -manifestNames Audit1
 -manifestPackage
"C:\Program Files (x86)\IBM\CaseManagement\solution_packages\Audit1.zip"
 -solutionName MySolution
```

Show the help for the exportSolutionAuditManifest command.
The following command shows the help for the **exportSolutionAuditManifest** command:

```
configmgr_cl exportSolutionAuditManifest -help
```

exportSolutionSecurityManifest command

The **exportSolutionSecurityManifest** command exports a case management security configuration from the development environment domain before you move the security configuration to another environment.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl exportSolutionSecurityManifest -profile myprofile
 -manifestNames manifest_names -manifestPackage manifest_package_file
 -solutionName solution_name [-silent] [-force] [-help]
```

Parameters

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-manifestNames *manifest_names*
Specifies the name of the security manifest. To specify more than one manifest at a time, enter multiple -manifestNames options with the command.

-manifestPackage *manifest_package_file*
Specifies the exported security package ZIP file. You can specify the full path and file name for the exported security package ZIP file. If the path includes spaces, put the entire path in double quotation marks. For example, enter "C:\Security Packages\Security1.zip".

If you specify only the file name, the security package is exported to the *ICM_Home*/CaseManagement/configure directory. If you do not specify an option for **-manifestPackage**, the security package is exported to *ICM_Home*/CaseManagement/solution_packages/*SolutionName*_securityManifest.zip.

-solutionName *solution_name*
Specifies the name of the solution that is associated with the security configuration.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Export a solution security configuration.

The following command exports the Security1 security configuration in the MyDevelop1 profile to the `Security1.zip` file:

```
configmgr_cl exportSolutionSecurityManifest -profile myDevelop1
 -manifestNames Security1
 -manifestPackage
"C:\Program Files (x86)\IBM\CaseManagement\solution_packages\Security1.zip"
 -solutionName MySolution
```

Show the help for the exportSolutionSecurityManifest command.

The following command shows the help for the **exportSolutionSecurityManifest** command:

```
configmgr_cl exportSolutionSecurityManifest -help
```

generateConfig command

The **generateConfig** command generates one or more configuration XML files for the specified configuration task to configure an IBM Case Manager application.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl generateConfig
 -deploy deploy_type content_management_type
 -box -db database_type -env environment_type
 -profileType profile_type -task task_type
 -taskfile task_file_name -taskname task_display_name
 -profile myprofile -form form_type
  [-silent] [-force] [-help]
```

Parameters

-deploy *deploy_type*

Specifies the type of IBM Case Manager deployment.

Table 34. Valid deploy_type values

Option	Description
`cluster`	Specify `cluster` if you are deploying IBM Case Manager to a web application server cluster.
`nd`	Specify `nd` for a network deployment of IBM Case Manager.
`standard`	Specify `standard` if you are deploying IBM Case Manager to a stand-alone web application server which is not managed or clustered.

The **-deploy** parameter is required only when you are generating all the files at the same time or when you are generating a single file by using one of the following **-taskfile** *task_file_name* options or **-task** *task_type* options:

Table 35. Deployment type is required to generate a single file by using these task options

-taskfile *task_file_name*	**-task** *task_type*
deploycaseapi.xml	deploycaseapi
deploycmbapp.xml	deploycmbapp
deployibmbpmis.xml	deployibmbpmis
deployregisterextensions.xml	deployregisterextensions
deployregisterwidgets.xml	deployregisterwidgets
deploycaseforms.xml	deploycaseforms

content_management_type
Specify -box for Box, -cm8 for IBM Content Manager or -bpm for IBM Business Process Manager.

-db *database_type*
Required only for the configibmcm option. This parameter specifies the type of database that IBM Content Manager uses. Choose a valid value from the following options:

Table 36. Valid database_type values

Environment	environment_type value
DB2	db2
Microsoft SQL Server	mssql
Oracle	oracle
Oracle Real Application Clusters (RAC)	oracle_rac

-env *environment_type*
Required only when you are generating all the files at the same time or for deploycaseforms.

Table 37. Valid environment_type values

Environment	environment_type value
Stand-alone Profile	standalone
Deployment Manager Profile	dmgr
Managed Profile	managed

-profileType *profile_type*
Indicates which type of profile to generate. The profile type determines which types of tasks can be generated. In general, you must generate and run all of the tasks for a profile type.

Table 38. Valid profile_type values

Option	Task files	Profile description
`wasdevelopmentenvironment`	If you create a full profile by omitting the **-task** *task_type* option, the profile includes a file for the application server properties, a file for Content Engine server properties, and a file for each task.	The development environment configuration profile prepares the development environment for creating, modifying, and testing solutions before moving them into a production domain.
	A WebSphere Application Server development environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configibmbpm.xml` • `configibmcm.xml` • `configrules.xml` • `createapps.xml` • `definedefaultprojectarea.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deploycmbapp.xml` • `deployibmbpmis.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registercpeapplets.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerprojectarea.xml` • `registerservices.xml` • `updatecpeclient.xml`	The profile includes the application server settings, Content Platform Engine server settings, and IBM Content Navigator settings. The profile can include one or more tasks.

Table 38. Valid profile_type values (continued)

Option	Task files	Profile description
`wasproductionenvironment`	If you create a full profile by omitting the **-task** *task_type* option, the profile includes a file for the application server properties, a file for Content Engine server properties, and a file for each task. A WebSphere Application Server production environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configibmbpm.xml` • `configibmcm.xml` • `configrules.xml` • `createapps.xml` • `definetargetenv.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deployibmbpmis.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `deploysolution.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registercpeapplets.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerservices.xml` • `registertargetenv.xml` • `updatecpeclient.xml`	The production environment configuration profile prepares the production environment for deploying solutions. The profile includes the application server settings, Content Platform Engine server settings, and IBM Content Navigator settings. The profile can include one or more tasks.

Table 38. Valid profile_type values (continued)

Option	Task files	Profile description
`wldevelopmentenvironment`	If you create a full profile by omitting the **-task** *task_type* option, the profile includes a file for the application server properties, a file for Content Engine server properties, and a file for each task.	The development environment configuration profile prepares the development environment for creating, modifying, and testing solutions before moving them into a production domain.
	An Oracle WebLogic Server development environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configrules.xml` • `createapps.xml` • `definedefaultprojectarea.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deploycmbapp.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registercpeapplets.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerprojectarea.xml` • `registerservices.xml` • `updatecpeclient.xml`	The profile includes the application server settings, Content Platform Engine server settings, and IBM Content Navigator settings. The profile can include one or more tasks.

Table 38. Valid profile_type values (continued)

Option	Task files	Profile description
`wlproductionenvironment`	If you create a full profile by omitting the **-task** *task_type* option, the profile includes a file for the application server properties, a file for Content Engine server properties, and a file for each task. An Oracle WebLogic Server production environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configrules.xml` • `createapps.xml` • `definetargetenv.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `deploysolution.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerservices.xml` • `registertargetenv.xml` • `updatecpeclient.xml`	The production environment configuration profile prepares the production environment for deploying solutions. The profile includes the application server settings, Content Platform Engine server settings, and IBM Content Navigator settings. The profile can include one or more tasks.

-task *task_type*
Indicates which task to generate. You can limit the tasks that are generated for a profile by using the **-task***task_type* option. You can omit the **-task** *task_type* parameter if you want to generate all the tasks or if you specify the **-taskfile** *task_file_name* parameter. The following table describes the valid task names, the associated configuration XML file, and a description of the settings that are affected by the task.

Table 39. Valid task_type values

Option	Description
No value is specified.	Use with the **-profileType** *profile_type* option to generate all of the tasks for the profile. If you omit the `-task` *task_type* parameter and the **-taskfile** *task_file_name* parameter, all the configuration files for the profile are generated. See the file list for the profile type in the table for the **-profileType** *type_of_profile* entry.
`configbox`	This task is required if you want to enable case workers to use Box to collaborate with external users. This task configures the connection to the Box server.

Table 39. Valid task_type values (continued)

Option	Description
`configcaseloginmodules`	Use with the **-profileType** *profile_type* option to generate the file for the task for configuring the login modules for the Case Manager Builder application. The login modules provide authentication information for the Case Manager Builder application. If you are deploying Case Manager Builder to the same application server where Content Engine is deployed, skip this task generation. This option generates the following file: `configcaseloginmodules.xml`
`configcmos`	Use with the **-profileType wasdevelopmentenvironment | wldevelopmentenvironment** option to generate the file for configuring the design and target object stores. This task installs the IBM Case Manager add-ons and creates the required events and subscriptions in Content Engine. This option generates the following file: `configcmos.xml`
`configibmbpm`	Use with the **-profileType** *profile_type* option to generate the file for configuring IBM Business Process Manager. This option generates the following file: `configibmbpm.xml`
`configibmcm`	Use with the **-profileType** *profile_type* option to generate the file for configuring IBM Content Manager. This option generates the following file: `configibmcm.xml`
`configrules`	Use with the **-profileType** *profile_type* option to generate the file for configuring business rules. This option generates the following file: `configrules.xml`

Table 39. Valid task_type values (continued)

Option	Description
`configureldap`	Use with the **-profileType** *profile_type* option to generate the file for configuring the directory service provider (LDAP) settings for the Case Manager Builder application. The directory service provider (LDAP) settings define the directory service and the users and groups that uses for authentication. If you have federated repositories and you must support multiple LDAP servers, create one additional file for each LDAP configuration. When you generate a second connection definition configuration file in the same profile, it is named `configureldap.2.xml`. The file name increments for each new file that you generate. You cannot change the file name, but you can edit the value in the file for the name of the task. This option generates the following files: `configureldap.xml` `configureldap.`*`n`*`.xml` . *n* is an integer starting with 2.
`createapps`	Use with the **-profileType** *profile_type* option to generate the file for updating the IBM Case Manager API WAR file and the Case Manager Builder EAR file with system parameters. This option generates the following file: `createapps.xml`
`definedefaultprojectarea`	Use with the **-profileType** *profile_type* option to generate the file for defining the default project area and the connection definition for the development environment target object store. This option generates the following file: `definedefaultprojectarea.xml`
`definetargetenv`	Use with the **-profileType** *profile_type* option to generate the file for defining the target environment and the connection definition for the production environment target object store. This option generates the following file: `definetargetenv.xml`
`deploycaseapi`	Use with the **-profileType wasdevelopmentenvironment | wldevelopmentenvironment** option to generate the file for deploying the IBM Case Manager API application on the web application server. Deploying the IBM Case Manager API application makes the application available for use by the Case Manager Builder or Case Manager Client application. This option generates the following file: `deploycaseapi.xml`

Table 39. Valid task_type values (continued)

Option	Description
`deploycaseforms`	Use with the **-profileType** *profile_type* option to generate the file for deploying forms applications. This option generates the following file: `deploycaseforms.xml`
`deploycmbapp`	Use with the **-profileType wasdevelopmentenvironment | wldevelopmentenvironment** option to generate the file for deploying a Case Manager Builder application instance on the web application server. Deploying makes the Case Manager Builder application available for use. This option generates the following file: `deploycmbapp.xml`
`deployibmbpmis`	Use with the **-profileType** *profile_type* option to generate the file for deploying IBM Business Process Manager. This option generates the following file: `deployibmbpmis.xml`
`deployregisterextension`	This task registers and deploys your extensions package.
`deployregisterwidgets`	Use with the **-profileType** *profile_type* option to generate the file for registering and deploying a widget package with Case Manager Builder and IBM Content Navigator. This option generates the following file: `deployregisterwidgets.xml`
`deploysolution`	Use with the **-profileType productionenvironment** option to generate the file for deploying an IBM Case Manager solution into a production target object store. You need one configuration file for each production environment target object store that you deploy a solution to. You can create additional task files in the same profile, or you can create a separate profile for the additional settings. When you generate a second solution deployment configuration file in a profile, it is named `deploysolution.2.xml`. The file name increments for each new file that you generate. You cannot change the file name, but you can edit the value in the file for the name of the task. This option generates the following files: `deploysolution.xml` `deploysolution.`*n*`.xml`. *n* is an integer starting with 2.
`registeradmin`	Use with the **-profileType** *profile_type* option to generate the file for registering the IBM Case Manager administration client with IBM Content Navigator. This option generates the following file: `registeradmin.xml`

Table 39. Valid task_type values (continued)

Option	Description
`registercpeapplets`	This task registers the plug-in for IBM Content Navigator that contains the Process Designer applet.
`registerexternaldataurl`	Use with the **-profileType** *profile_type* option to generate the file that registers a data source other than Content Platform Engine. This option generates the following file: `registerexternaldataurl.xml`
`registerprojectarea`	Use with the **-profileType** *profile_type* option to generate the file for registering the project area with IBM Content Navigator and configures the Content Platform Engine repositories. This option generates the following file: `registerprojectarea.xml`
`registertargetenv`	Use with the **-profileType** *profile_type* option to generate the file for registering the target environment with IBM Content Navigator and configures the Content Platform Engine repositories. This option generates the following file: `registertargetenv.xml`
`registerexternaldataurl`	Use with the **-profileType** *profile_type* option to generate the file for registering an external data source URL with IBM Case Manager. This option generates the following file: `registerexternaldataurl.xml`
`registericmmonitor`	This task imports and registers the Case Monitor widgets package with the IBM Case Manager server, registers the plug-in for the widgets package with the IBM Content Navigator server, and creates the Case Monitor desktop. This task is required to enable Case Monitor. Save your changes and run the task to apply your settings. In a cluster environment, you must either use the IBM Content Navigator administration client to manually load the plug-in inside of the extensions package on each node or restart the application server cluster to force all nodes to load the plug-in. Before using Case Monitor, you must create a Case Analyzer store for each case management target object store.
`registerprojectarea`	This task registers a project area with an IBM Case Manager desktop, creates default IBM Case Manager desktops, configures repositories for the case management design and target object stores, and adds IBM Case Manager features to the desktop. Also, this task configures the Case Operations component queue and configures the project area's isolated region to work with solution workflows. This task is required and must be run for every project area.

Table 39. Valid task_type values (continued)

Option	Description
`registerservices`	This task registers the plug-in for IBM Content Navigator that contains the IBM Case Manager services that are used by other components.
`updatecpeclient`	Use with the **-profileType** *profile_type* option to generate the file for updating the client connector files for Content Platform Engine. This option generates the following file: `updatecpeclient.xml`

-taskfile *task_file_name*
Specifies the *configuration*`.xml file` to use.

If only one task file exists for the *task_type*, the **-taskfile** *task_file_name* parameter is optional.

If more than one task file for the *task_type* exists, you must include the **-taskfile** *task_file_name* parameter. The *task_file* value is case sensitive if your operating system is case sensitive for file names.

-taskname *task_display_name*
Specifies the task display name. Use this option with the **-task** *task_type* or **-taskfile** *task_file_name* to provide a custom display name for the task. If you omit this parameter, a default display name is used. When you configure multiple tasks of the same type (for example, multiple deploysolution tasks), ensure that you enter descriptive display names for each task.

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*`/CaseManagement/configure/profiles` directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1"` or `/opt/IBM/CaseManagement/configure/profiles/develop1`.
- The full path to the profile input file, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp"` or `/opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp`.

-form *form_type*
Specifies the form type to integrate with IBM Case Manager. If you specify `ibmforms`, IBM Case Manager will be configured to use eForms and IBM Forms. The *form_type* value can be one of the following items:

- `eforms`
- `ibmforms`

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Generate all configuration files at the same time for a profile.
The following command generates all the configuration XML files for a new development environment configuration profile for a standard deployment with IBM Tivoli Directory Server that uses a stand-alone LDAP repository in the *install_path*/CaseManagement/configure/profiles/Develop1 directory:

```
configmgr_cl generateConfig
 -deploy standard
 -db db2 -env standalone
 -profileType wasdevelopmentenvironment
 -profile Develop1
```

Generate only the deploysolution task file.
The following command generates only the deploysolution.xml file for a production environment profile in the *install_path*/CaseManagement/configure/profiles/Production1 directory:

```
configmgr_cl generateConfig
 -profileType wasproductionenvironment
 -task deploysolution -profile Production1
```

If a deploysolution.xml file is already in the profile directory, the file name is incremented, for example, deploysolution.2.xml.

Generate only the deploysolution task file and provide a display name for the task.
The following command generates only the deploysolution.xml file for a case deployment profile in the *install_path*/CaseManagement/configure/profiles/Production1 directory and uses a display name of Deploy to object store ObjectStore2:

```
configmgr_cl generateConfig
 -profileType wasproductionenvironment
 -task deploysolution  -profile ObjectStore2
 -taskname "Deploy to object store ObjectStore2"
```

Show the help for the generateConfig command.
The following command shows the help for the **generateConfig** command:

```
configmgr_cl generateConfig -help
```

Related tasks:

Configuration checklist

generate_input_sa command

The **generate_input_sa** command generates the input file for copying a solution, creating a solution from a template, converting a solution to a template, or listing the properties and document types in an object store.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl generate_input_sa -operation operation_type
 -file input_file_name
 [-silent] [-force] [-help]
```

Parameters

-operation *operation_type*

Indicates the operation type that you will use the input file with. The values in the input file depend on the operation that you use the file with.

Table 40. Valid operation_type values

Option	Description
`copy`	Creates the input file for copying a solution.
`createFromTemplate`	Creates the input file for creating a solution from a template.
`list`	Creates the input file for listing the properties and document types in an object store.
`convertToTemplate`	Converts a solution to a template.

-file *input_file_name*

Specifies the full path to the input file to create. The directory structure in the path must already exist. You can use any valid file name, but the `.txt` extension is recommended. For example, use `C:\propertylist\propertylist.txt`.

-silent

Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force

Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help

Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Generate the input file for creating a list of properties and document types.

The following command generates the `C:\propertylist\propertylist.txt` text file for creating a list of properties and document types:

```
configmgr_cl generate_input_sa -operation list
 -file C:\propertylist\propertylist.txt
```

Generate the input file for copying a solution.

The following command generates the `C:\solutions\copy_solution_input.txt` input file for creating a list of properties and document types:

```
configmgr_cl generate_input_sa -operation copy
 -file C:\solutions\copy_solution_input.txt
```

Show the help for the generate_input_sa command.

The following command shows the help for the **generate_input_sa** command:

```
configmgr_cl generate_input_sa -help
```

Related reference:

"**execute_sa** command" on page 341

generateObjectStoreDataMap command

The **generateObjectStoreDataMap** command generates the object store data map for mapping the object stores that are contained in a solution package to the appropriate object stores in the target environment.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl generateObjectStoreDataMap
 -solutionPackage package_file
 -file datamap_file
  [-silent][-force][-help]
```

Parameters

-solutionPackage *package_file*

Specifies the full path and file name of the solution package for which you are creating the data map. If the path includes spaces, put the entire path in double quotation marks. For example, enter `"C:\Solution Packages\Credit Dispute Solution.zip"`.

-file *datamap_file*

Specifies the full path and file name for the data map file to create. The directory structure in the path must already exist. You can use any valid file name, but the .xml extension is recommended. If the path includes a directory name with spaces, put the entire path in double quotation marks. For example, enter `"C:\Solution Packages\datamap.xml"`.

-help

Optional and displays a brief message on the command syntax instead of running the command.

generateServiceDataMap command

The **generateServiceDataMap** command creates the service data map XML file for importing a solution or solution template into another environment.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl generateServiceDataMap
 -solutionPackage package_file
 -file service_data_map_name
[-silent] [-force] [-help]
```

Parameters

-solutionPackage *package_file*
Specifies the full path and file name the solution package ZIP file that contains the solution to import. If the path includes spaces, put the entire path in double quotation marks. For example, enter `"C:\Solution Packages\Credit Dispute Solution.zip"`.

-file *service_data_map_name*
Specifies the full path and file name for the service data map XML file to create. The directory structure in the path must already exist. You can use any valid file name, but the .xml extension is recommended. If the path includes a directory name with spaces, enclose the entire path in double quotation marks. For example, enter `"C:\Solution Packages\sevice_data_map.xml"`.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Create the service datamap file for a solution package.
The following command generates the service data mapping file for the `Credit Dispute Solution.zip` solution package:

```
configmgr_cl generateServiceDataMap
 -solutionPackage "C:\Solution Packages\Credit Dispute Solution.zip"
 -file "C:\Solution Packages\sevice_data_map.xml"
```

Show the help for the generateServiceDataMap command.
The following command shows the help for the **generateServiceDataMap** command:

```
configmgr_cl generateServiceDataMap -help
```

Related reference:

"**importSolution** command" on page 375

generateUpgrade command

The **generateUpgrade** command generates a new profile for upgrading an existing installation of IBM Case Manager. If a source profile is specified, the command copies all relevant tasks and properties from the source profile to the new upgrade profile. If a profile is specified that does not exist, a profile is created with all required tasks for upgrading an existing installation of IBM Case Manager.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl generateUpgrade content_management_type
 -db database_type -deploy deploy_type
 -env environment_type -form form_type
 -profileType profile_type -profile myprofile
 -source source_profile
 [-force] [-help]
```

Parameters

content_management_type

Specify `-cm8` for IBM Content Manager or `-bpm` for IBM Business Process Manager.

-db *database_type*

Required only for the `configibmcm` option. This parameter specifies the type of database that IBM Content Manager uses. Choose a valid value from the following options:

Table 41. Valid database_type values

Environment	environment_type value
DB2	`db2`
Microsoft SQL Server	`mssql`
Oracle	`oracle`
Oracle Real Application Clusters (RAC)	`oracle_rac`

-deploy *deploy_type*

Specifies the type of IBM Case Manager deployment.

Table 42. Valid deploy_type values

Option	Description
`cluster`	Specify `cluster` if you are deploying IBM Case Manager to a web application server cluster.
`nd`	Specify `nd` for a network deployment of IBM Case Manager.
`standard`	Specify `standard` if you are deploying IBM Case Manager to a stand-alone web application server which is not managed or clustered.

The **-deploy** parameter is required only when you are generating all the files at the same time or when you are generating a single file by using one of the following **-taskfile** *task_file_name* options or **-task** *task_type* options:

Table 43. Deployment type is required to generate a single file by using these task options

-taskfile *task_file_name*	**-task** *task_type*
deploycaseapi.xml	deploycaseapi
deploycmbapp.xml	deploycmbapp
deployibmbpmis.xml	deployibmbpmis
deployregisterextensions.xml	deployregisterextensions
deployregisterwidgets.xml	deployregisterwidgets
deploycaseforms.xml	deploycaseforms

-env *environment_type*
Required only when you are generating all the files at the same time or for deploycaseforms.

Table 44. Valid environment_type values

Environment	environment_type value
Stand-alone Profile	standalone
Deployment Manager Profile	dmgr
Managed Profile	managed

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-form *form_type*
Specifies the form type to integrate with IBM Case Manager. If you specify ibmforms, IBM Case Manager will be configured to use eForms and IBM Forms. The *form_type* value can be one of the following items:

- eforms
- ibmforms

-help
Optional: Shows a brief message on the command syntax instead of running the command.

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-profileType *profile_type*
Indicates which type of profile to generate. The profile type determines which types of tasks can be generated. In general, you must generate and run all of the tasks for a profile type.

Table 45. Valid profile_type values

Option	Task files	Profile description
`wasdevelopmentenvironment`	If you create a full profile by omitting the **-task** *task_type* option, the profile includes a file for the application server properties, a file for Content Engine server properties, and a file for each task.	The development environment configuration profile prepares the development environment for creating, modifying, and testing solutions before moving them into a production domain.
	A WebSphere Application Server development environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configibmbpm.xml` • `configibmcm.xml` • `configrules.xml` • `createapps.xml` • `definedefaultprojectarea.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deploycmbapp.xml` • `deployibmbpmis.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registercpeapplets.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerprojectarea.xml` • `registerservices.xml` • `updatecpeclient.xml`	The profile includes the application server settings, Content Platform Engine server settings, and IBM Content Navigator settings. The profile can include one or more tasks.

Table 45. Valid profile_type values (continued)

Option	Task files	Profile description
`wasproductionenvironment`	If you create a full profile by omitting the **-task** *task_type* option, the profile includes a file for the application server properties, a file for Content Engine server properties, and a file for each task. A WebSphere Application Server production environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configibmbpm.xml` • `configibmcm.xml` • `configrules.xml` • `createapps.xml` • `definetargetenv.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deployibmbpmis.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `deploysolution.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registercpeapplets.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerservices.xml` • `registertargetenv.xml` • `updatecpeclient.xml`	The production environment configuration profile prepares the production environment for deploying solutions. The profile includes the application server settings, Content Platform Engine server settings, and IBM Content Navigator settings. The profile can include one or more tasks.

Table 45. Valid profile_type values (continued)

Option	Task files	Profile description
`wldevelopmentenvironment`	If you create a full profile by omitting the **-task** *task_type* option, the profile includes a file for the application server properties, a file for Content Engine server properties, and a file for each task.	The development environment configuration profile prepares the development environment for creating, modifying, and testing solutions before moving them into a production domain.
	An Oracle WebLogic Server development environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configrules.xml` • `createapps.xml` • `definedefaultprojectarea.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deploycmbapp.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registercpeapplets.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerprojectarea.xml` • `registerservices.xml` • `updatecpeclient.xml`	The profile includes the application server settings, Content Platform Engine server settings, and IBM Content Navigator settings. The profile can include one or more tasks.

Table 45. Valid profile_type values (continued)

Option	Task files	Profile description
`wlproductionenvironment`	If you create a full profile by omitting the **-task** *task_type* option, the profile includes a file for the application server properties, a file for Content Engine server properties, and a file for each task. An Oracle WebLogic Server production environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configrules.xml` • `createapps.xml` • `definetargetenv.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `deploysolution.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerservices.xml` • `registertargetenv.xml` • `updatecpeclient.xml`	The production environment configuration profile prepares the production environment for deploying solutions. The profile includes the application server settings, Content Platform Engine server settings, and IBM Content Navigator settings. The profile can include one or more tasks.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-source ***source_profile***
Specifies the full path to the directory where the source profile is located. If the path includes a directory name with spaces, enclose the entire path in double quotation marks. For example, enter `"C:\Program Files\profiles\develop1"`.

gui command

The **gui** command opens the IBM Case Manager configuration tool graphical user interface. The graphical user interface presents the same functions as the command-line version, but with dialogs and fields for editing the properties and settings.

Syntax

```
configmgr_cl gui
```

Example

The following command starts the IBM Case Manager configuration tool graphical user interface:

```
configmgr_cl gui
```

importProps command

The **importProps** command imports properties values from a task in an existing configuration profile into a similar task in another profile. Importing existing values saves time when you are reusing information across profiles.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl importProps  -source source_profile
 -sourceTask task_type | -sourceTaskName task_name
 -target target_profile
 -targetTask task_type | -targetTaskName task_name
 [-silent] [-force] [-help]
```

Parameters

-source *source_profile*

Specifies the full path to the directory where the source profile is located. Property values will be imported from this profile. If the path includes a directory name with spaces, enclose the entire path in double quotation marks. For example, enter `"C:\Program Files\profiles\develop1"`.

-sourceTask *task_type*

Specifies the type of task that you want to import values from. If you specify the **sourceTask** *task_type* parameter, you can omit the **-sourceTaskName** *task_type* parameter.

Table 46. Valid task_type and task_name values

Task type option	Default task display name	Description
`configcaseloginmodules`	Configure the Login Modules	Imports the properties from the task that configures the login modules for the Case Manager Builder application. The login modules provide authentication information for the Case Manager Builder application. The properties are stored in the `configcaseloginmodules.xml` file.
`configbox`	Configure Box Collaboration	This task is required if you want to enable case workers to use Box to collaborate with external users. This task configures the connection to the Box server.
`configcmos`	Configure the Case Management Object Stores	Imports the properties from the task that configures the development environment design and target object stores. This task installs the IBM Case Manager Add-ons and creates the required events and subscriptions in Content Engine. The properties are stored in the `configcmos.xml` file.

Table 46. Valid task_type and task_name values (continued)

Task type option	Default task display name	Description
`configibmbpm`	Configure IBM Business Process Manager	Imports the properties from the task that configures the connection to the IBM Business Process Manager host server. This task is required if you use IBM Business Process Manager as the workflow server for IBM Case Manager.
`configibmcm`	Configure IBM Content Manager	This task configures the connection to the IBM Content Manager host server. This task is required if you use IBM Content Manager as the content repository for IBM Case Manager.
`configrules`	Configure Business Rules	Imports the properties from the task that configures Business Rules for your environment and configures the Rules Operations component queue. This task is optional. You must run the Register Target Environment task before you run this task.
`configureldap`	Configure LDAP	Imports the properties from the task that configures the directory service provider (LDAP) settings for the Case Manager Builder application. The directory service provider (LDAP) settings define the directory service and the users and groups that uses for authentication. The properties are stored in the following files: `configureldap.xml` `configureldap.`*`n`*`.xml` . *n* is an integer starting with 2.
`contentengineserver`	Content Platform Engine	Content Platform Engine settings that are common to all tasks in the profile. These settings are used when you run any of the tasks for the production environment profile. The properties include the Content Platform Engine domain information, the case management design object store name, and other information about the production environment.
`contentnavigatorserver`	IBM Content Navigator	IBM Content Navigator settings that are common to all tasks in the profile. These settings are used when you run some of the tasks for the production environment profile. The properties include the IBM Content Navigator server installation directory, the administrative user name and password, the port number, cell, and other information about IBM Content Navigator.

Table 46. Valid task_type and task_name values (continued)

Task type option	Default task display name	Description
`createapps`	Create Case Manager Applications	Imports the properties from the task that adds the Content Platform Engine EJB URL and timeout values to the IBM Case Manager API WAR file, adds the location of the help topics to the IBM Case Manager help system WAR file, and configures the IBM Case Manager Forms WAR file for FileNet eForms or IBM Forms. You must run this task before you run the Deploy the Case Manager API WAR task, the Deploy Case Manager Help System task, or the Deploy the Forms Application task. If you change the location of your network shared directory after you run this task, you must run this task again and redeploy the IBM Case Manager help system WAR file.
`definedefaultprojectarea`	Define the Default Project Area	Imports the properties from the task that defines the default project area for the development environment. A project area groups solutions in the design object store so that the entire object store is not affected when you reset the test environment. Only users who are assigned to a project area can log on to Case Manager Builder. The default project area is required for each development environment.
`definetargetenv`	Define Target Environment	Imports the properties from the task that defines a target environment for the production environment. A case management solution is deployed to a target environment. A target environment consists of a connection point and an object store, and is associated with one or more IBM Content Navigator desktops. A unique target environment is required for every connection point that will be used for solution deployment. This task is required.
`deploycaseapi`	Deploy the IBM Case Manager API	Imports the properties from the task that deploys the IBM Case Manager API application on the web application server. Deploying the IBM Case Manager API application makes the application available for use by the IBM Case Manager application. The properties are stored in the `deploycaseapi.xml` file.

Table 46. Valid task_type and task_name values (continued)

Task type option	Default task display name	Description
`deploycaseforms`	Deploy the Forms Application	Imports the properties from the task that integrates forms into your case management configuration. This task is required. You must run the Create the Case Manager Applications task before you run this task. If you are integrating with IBM Forms on a stand-alone server, you must restart your application server after you run this task. If you are integrating with IBM Forms on a network deployment or cluster, you must first deploy the application against the deployment manager, run the task against each managed node, then restart your managed node or cluster after running the task on all managed nodes. If you do not use IBM Forms, you are not required to restart the application server.
`deploycmbapp`	Deploy Case Manager Builder	Imports the properties from the task that deploys a Case Manager Builder instance on the web application server. Deploying makes the Case Manager Builder application available for use. The properties are stored in the `deploycmbapp.xml` file.
`deployibmbpmis`	Deploy the IBM Business Process Manager Integration Service	The IBM Business Process Manager integration service provides immediate workflow status to the IBM Case Manager server. This task configures the communication between the Content Platform Engine server and the IBM Business Process Manager server. This task is required if you use IBM Business Process Manager as the workflow server for IBM Case Manager.
`deployregisterextensions`	Deploy and Register Extensions Package	This task registers and deploys your extensions package.
`deployregisterwidgets`	Deploy and Register Widgets Package	Imports the properties from the task that registers the widgets package with the IBM Case Manager server, registers the plug-in for the widgets package with the IBM Content Navigator server, and deploys the EAR file in the widgets package to the web application server, if present. This task is required for the default widgets package that comes with IBM Case Manager. You can also run this task to register your custom widgets packages.
`deploysolution`	Deploy Solution	Imports the properties from the task that deploys an IBM Case Manager solution into a production target object store. The properties are stored in the following files: `deploysolution.xml` `deploysolution.`*`n`*`.xml`. *n* is an integer starting with 2.

Table 46. Valid task_type and task_name values (continued)

Task type option	Default task display name	Description
`registerboxlistener`	Register the IBM Case Manager Box Event Listener Plug-in	This task registers the plug-in for IBM Content Navigator that listens for case-related Box events when Box collaboration is enabled. This task is required if you want Box events to trigger the creation of cases or work items. Save your changes and run the task to apply your settings.
`registercpeapplets`	Register the IBM Content Platform Engine Applets Support Plug-in	This task registers the plug-in for IBM Content Navigator that contains the Process Designer applet.
`registerexternaldataurl`	Register the External Data Service	This task creates a connection to an external data service, which allows you to use data in a solution from a source other than Content Platform Engine. This task is required only if you are using an external data service in a solution.
`registerprojectarea`	Register Project Area	Imports the properties from the task registers a project area with an IBM Content Navigator desktop, creates the default IBM Case Manager desktops, configures the repositories for the case management design and target object stores, and adds IBM Case Manager features to the desktop. Also, this task configures the Case Operations component queue and configures the project area's isolated region to work with solution workflows. This task is required and must be run for every project area. You must run the Deploy and Register Widgets Package task and the Register the IBM Case Manager Administration Client Plug-in task before you run this task.
`registerservices`	Register the IBM Case Manager Services Plug-in	Imports the properties from the task that registers the plug-in for IBM Content Navigator that contains the IBM Case Manager services that are used by other components. This task is required.
`registertargetenv`	Register Target Environment	Imports the properties from the task registers a target environment with an IIBM Content Navigator desktop, creates the default IBM Case Manager desktops, configures the repositories for the case management design and target object stores, and adds IBM Case Manager features to the desktop. Also, this task configures the Case Operations component queue and configures the target environment's isolated region to work with solution workflows. This task is required and must be run for every target environment. You must run the Deploy and Register Widgets Package task and the Register the IBM Case Manager Administration Client Plug-in task before you run this task.

Table 46. Valid task_type and task_name values (continued)

Task type option	Default task display name	Description
`updatecpeclient`	Update the Content Platform Engine Client Connector files	Imports the properties from the task that downloads the correct version of the Content Platform Engine Client Connector files.
`websphereapplicationserver` or `weblogicapplicationserver`	Application server	Application server settings that are common to all tasks in the profile. These settings are used when you run any of the tasks for the production environment profile. The properties include the application server installation directory, the administrative user name and password, the port number, cell, and other information about the application server. Each profile contains only one of these files, depending on the application server type.
`registericmmonitor`	Register the Case Monitor Widgets Package	This task imports and registers the Case Monitor widgets package with the IBM Case Manager server, registers the plug-in for the widgets package with the IBM Content Navigator server, and creates the Case Monitor desktop. This task is required to enable Case Monitor. Save your changes and run the task to apply your settings. In a cluster environment, you must either use the IBM Content Navigator administration client to manually load the plug-in inside of the extensions package on each node or restart the application server cluster to force all nodes to load the plug-in. Before using Case Monitor, you must create a Case Analyzer store for each case management target object store.

-sourceTaskName *task_name*

Specifies the display name for the task that you want to import values from. If you specify the **sourceTask** *task_type* parameter, you can omit the **-sourceTaskName** *task_type* parameter.

If the display name includes spaces, you must use quotation marks around the display name, as in the following example:

```
-sourceTaskName "Configure LDAP"
```

-target *target_profile*

Specifies the full path to the directory where the target profile is located. The values will be imported into this profile.

-targetTask *task_type*

Specifies the type of task that you want to import values to. If you specify the **targetTask** *task_type* parameter, you can omit the **-targetTaskName** *task_type* parameter.

See the "Valid task_type and task_name values" table for a list of valid *task_type* values.

-targetTaskName *task_name*

Specifies the display name for the task that you want to import values to. If you specify the **targetTask** *task_type* parameter, you can omit the **-targetTaskName** *task_type* parameter.

See the "Valid task_type and task_name values" table for a list of valid *task_name* values.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Import the properties by specifying the task type.
The following command imports the properties for the configure LDAP task from the builder1 profile into the configure LDAP task for the develop1 profile:

```
configmgr_cl importProps
 -source
"C:\Program Files\IBM\CaseManagement\configure\profiles\builder1"
 -sourceTask configureldap
 -target
"C:\Program \IBM\CaseManagement\configure\profiles\develop1"
 -targetTask configureldap
```

Import the properties by specifying the display name.
The following command imports the properties for the task with the display name “Deploy Case Manager Client” from the client2 profile into the “Deploy Case Manager Client” task for the develop1 profile:

```
configmgr_cl importProps
 -source
"C:\Program Files\IBM\CaseManagement\configure\profiles\client2"
 -sourceTaskName "Deploy Case Manager Client"
 -target
"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1"
 -targetTaskName "Deploy Case Manager Client"
```

Show the help for the importProps command.
The following command shows the help for the **importProps** command:

```
configmgr_cl importProps -help
```

Related tasks:

“Exporting other FileNet P8 assets” on page 135

Related reference:

"**listImportTargetTasks** command" on page 380

importSolution command

The **importSolution** command imports a case management solution or solution template package into another environment.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl importSolution -profile myprofile
 -solutionPackage package_file
 -projectAreaName project_area_name
 -serviceDataMap service_data_map_name
 -objectStoreDataMap object_store_data_map_name
 [-silent] [-force] [-help]
```

Parameters

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-solutionPackage *package_file*
Specifies the full path and file name the solution package ZIP file that conatins the solution to import. If the path includes spaces, put the entire path in double quotation marks. For example, enter "C:\Solution Packages\Credit Dispute Solution.zip".

-projectAreaName *project_area_name*
Specifies the name of the project area for the solution. This option is valid only for importing a solution package to into another development environment.

-serviceDataMap *service_data_map_name*
Specifies the full path and file name for the service data map XML file that was generated by using the **generateServiceDataMap** command or by using FileNet Deployment Manager. If the path includes a directory name with spaces, enclose the entire path in double quotation marks. For example, enter "C:\\Solution Packages\\sevice_data_map.xml".

-objectStoreDataMap *object_store_data_map_name*
Specifies the full path and file name for the object store data map XML file that was generated by using the **generateObjectStoreDataMap** command or by using FileNet Deployment Manager. If the path includes a directory name with spaces, enclose the entire path in double quotation marks. For example, enter "C:\Solution Packages\object_store_data_map.xml".

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to

the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Import a solution package by using the default service datamap.
The following command imports the `Solution1.zip` solution package to the object store that is used in the MyDevelop1 profile. The solution will be assigned to the Credit Dispute project area. The default data mapping is used.

```
configmgr_cl importSolution -profile myDevelop1
 -solutionPackage "C:\solution packages\Solution1.zip"
 -projectArea "Credit Dispute"
```

Import a solution package by using custom service datamap.
The following command imports the `Solution1.zip` solution package to the object store that is used in the MyDevelop1 profile. The solution will be assigned to the Credit Dispute project area. A custom datamap that was created with the **generateServiceDataMap** command is used.

```
configmgr_cl importSolution -profile myDevelop1
 -solutionPackage "C:\solution packages\Solution1.zip"
 -projectArea "Credit Dispute"
 -serviceDataMap "C:\solution packages\sevice_data_map.xml"
```

Show the help for the importSolution command.
The following command shows the help for the **importSolution** command:

```
configmgr_cl importSolution -help
```

Related reference:

"**generateServiceDataMap** command" on page 360

importSolutionAuditManifest command

The **importSolutionAuditManifest** command imports an audit configuration package from one environment into another environment.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl importSolutionAuditManifest -profile myprofile
 -manifestPackage manifest_package_file
 [-silent] [-force] [-help]
```

Parameters

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-manifestPackage *manifest_package_file*
Specifies the full path and file name of the audit configuration package ZIP file. If the path includes spaces, put the entire path in double quotation marks. For example, enter "C:\Audit Packages\Audit1.zip".

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Import an audit configuration package.
The following command imports the Audit1.zip audit configuration package file in the Profile1 profile.

```
configmgr_cl importSolutionAuditManifest -profile Profile1
 -manifestPackage Audit1.zip
 [-silent] [-force] [-help]
```

Show the help for the importSolutionAuditManifest command.
The following command shows the help for the **importSolutionAuditManifest** command:

```
configmgr_cl importSolutionAuditManifest -help
```

importSolutionManifest command

The **importSolutionManifest** command imports a case management solution from a version control system into another environment by using a manifest and a set of files.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl importSolutionManifest -profile myprofile
 -solutionManifest mymanifest
 -projectAreaName project_area_name
 [-silent] [-force] [-help]
```

Parameters

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-solutionManifest *mymanifest*
The full path to the solution manifest that you want to import.

If the path includes a directory name with spaces, enclose the path in double quotation marks. For example, enter "C:\Solution Manifests\SOL1_Manifest.json".

Any files that are related to the solution manifest must be in the same folder as the solution manifest.

-projectAreaName *project_area_name*
Specifies the name of the project area for the solution. This option is valid only for importing a solution package to into another development environment.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Import a solution package to a development environment by using a solution manifest.

The following command imports the solution package that is identified by the SOL1 manifest to the object store that is used in the MyDevelop1 profile. The solution will be assigned to the Credit Dispute project area. This command also imports the SOL1 files that were extracted to the same folder as the SOL1 manifest.

```
configmgr_cl importSolutionManifest -profile myDevelop1
 -solutionManifest "C:\Solution Manifests\SOL1_Manifest.json"
 -projectArea "Credit Dispute"
```

Show the help for the importSolutionManifest command.

The following command shows the help for the **importSolutionManifest** command:

```
configmgr_cl importSolutionManifest -help
```

importSolutionSecurityManifest command

The **importSolutionSecurityManifest** command imports a security configuration package from one environment into another environment.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl importSolutionSecurityManifest -profile myprofile
 -manifestPackage manifest_package_file
 [-silent] [-force] [-help]
```

Parameters

-profile *myprofile*

Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-manifestPackage *manifest_package_file*

Specifies the full path and file name of the security configuration package ZIP file. If the path includes spaces, put the entire path in double quotation marks. For example, enter "C:\Security Packages\Security1.zip".

-silent

Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force

Optional and applies only when the **-silent** parameter is used. When you

specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Import a security configuration package.
The following command imports the `Security1.zip` security configuration package file in the Profile1 profile.

```
configmgr_cl importSolutionSecurityManifest -profile Profile1
 -manifestPackage Security1.zip
 [-silent] [-force] [-help]
```

Show the help for the importSolutionSecurityManifest command.
The following command shows the help for the **importSolutionSecurityManifest** command:

```
configmgr_cl importSolutionSecurityManifest -help
```

listImportTargetTasks command

The **listImportTargetTasks** command displays a preview of the task mapping before you import properties values from an existing configuration profile into another profile. The command lists the source and target profiles, the source and target task types, the display name of the tasks, and whether a new task will be created.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl listImportTargetTasks  -source source_profile
 -sourceTask task_type | -sourceTaskName task_name
 -target target_profile
 [-help]
```

Parameters

-source *source_profile*
Specifies the full path to the directory where the source profile is located. Property values will be imported from this profile. If the path includes a directory name with spaces, enclose the entire path in double quotation marks. For example, enter `"C:\Program Files\profiles\develop1"`.

-source *source_profile*
Specifies the full path to the directory where the source profile is located. Property values will be imported from this profile when you use the **importProps** command.

-sourceTask *task_type*

Specifies the type of task that you want to import values from. If you specify the **sourceTask** *task_type* parameter, you can omit the **-sourceTaskName** *task_type* parameter.

Table 47. Valid task_type and task_name values

Task type option	Default task display name	Description
`configcaseloginmodules`	Configure the Login Modules	Imports the properties from the task that configures the login modules for the Case Manager Builder application. The login modules provide authentication information for the Case Manager Builder application. The properties are stored in the `configcaseloginmodules.xml` file.
`configbox`	Configure Box Collaboration	This task is required if you want to enable case workers to use Box to collaborate with external users. This task configures the connection to the Box server.
`configcmos`	Configure the Case Management Object Stores	Imports the properties from the task that configures the development environment design and target object stores. This task installs the IBM Case Manager Add-ons and creates the required events and subscriptions in Content Engine. The properties are stored in the `configcmos.xml` file.
`configibmbpm`	Configure IBM Business Process Manager	Imports the properties from the task that configures the connection to the IBM Business Process Manager host server. This task is required if you use IBM Business Process Manager as the workflow server for IBM Case Manager.
`configibmcm`	Configure IBM Content Manager	This task configures the connection to the IBM Content Manager host server. This task is required if you use IBM Content Manager as the content repository for IBM Case Manager.
`configrules`	Configure Business Rules	Imports the properties from the task that configures Business Rules for your environment and configures the Rules Operations component queue. This task is optional. You must run the Register Target Environment task before you run this task.
`configureldap`	Configure LDAP	Imports the properties from the task that configures the directory service provider (LDAP) settings for the Case Manager Builder application. The directory service provider (LDAP) settings define the directory service and the users and groups that uses for authentication. The properties are stored in the following files: `configureldap.xml` `configureldap.`*`n`*`.xml` . *n* is an integer starting with 2.

Table 47. Valid task_type and task_name values (continued)

Task type option	Default task display name	Description
`contentengineserver`	Content Platform Engine	Content Platform Engine settings that are common to all tasks in the profile. These settings are used when you run any of the tasks for the production environment profile. The properties include the Content Platform Engine domain information, the case management design object store name, and other information about the production environment.
`contentnavigatorserver`	IBM Content Navigator	IBM Content Navigator settings that are common to all tasks in the profile. These settings are used when you run some of the tasks for the production environment profile. The properties include the IBM Content Navigator server installation directory, the administrative user name and password, the port number, cell, and other information about IBM Content Navigator.
`createapps`	Create Case Manager Applications	Imports the properties from the task that adds the Content Platform Engine EJB URL and timeout values to the IBM Case Manager API WAR file, adds the location of the help topics to the IBM Case Manager help system WAR file, and configures the IBM Case Manager Forms WAR file for FileNet eForms or IBM Forms. You must run this task before you run the Deploy the Case Manager API WAR task, the Deploy Case Manager Help System task, or the Deploy the Forms Application task. If you change the location of your network shared directory after you run this task, you must run this task again and redeploy the IBM Case Manager help system WAR file.
`definedefaultprojectarea`	Define the Default Project Area	Imports the properties from the task that defines the default project area for the development environment. A project area groups solutions in the design object store so that the entire object store is not affected when you reset the test environment. Only users who are assigned to a project area can log on to Case Manager Builder. The default project area is required for each development environment.
`definetargetenv`	Define Target Environment	Imports the properties from the task that defines a target environment for the production environment. A case management solution is deployed to a target environment. A target environment consists of a connection point and an object store, and is associated with one or more IBM Content Navigator desktops. A unique target environment is required for every connection point that will be used for solution deployment. This task is required.

Table 47. Valid task_type and task_name values (continued)

Task type option	Default task display name	Description
`deploycaseapi`	Deploy the IBM Case Manager API	Imports the properties from the task that deploys the IBM Case Manager API application on the web application server. Deploying the IBM Case Manager API application makes the application available for use by the IBM Case Manager application. The properties are stored in the `deploycaseapi.xml` file.
`deploycaseforms`	Deploy the Forms Application	Imports the properties from the task that integrates forms into your case management configuration. This task is required. You must run the Create the Case Manager Applications task before you run this task. If you are integrating with IBM Forms on a stand-alone server, you must restart your application server after you run this task. If you are integrating with IBM Forms on a network deployment or cluster, you must first deploy the application against the deployment manager, run the task against each managed node, then restart your managed node or cluster after running the task on all managed nodes. If you do not use IBM Forms, you are not required to restart the application server.
`deploycmbapp`	Deploy Case Manager Builder	Imports the properties from the task that deploys a Case Manager Builder instance on the web application server. Deploying makes the Case Manager Builder application available for use. The properties are stored in the `deploycmbapp.xml` file.
`deployibmbpmis`	Deploy the IBM Business Process Manager Integration Service	The IBM Business Process Manager integration service provides immediate workflow status to the IBM Case Manager server. This task configures the communication between the Content Platform Engine server and the IBM Business Process Manager server. This task is required if you use IBM Business Process Manager as the workflow server for IBM Case Manager.
`deployregisterextensions`	Deploy and Register Extensions Package	This task registers and deploys your extensions package.
`deployregisterwidgets`	Deploy and Register Widgets Package	Imports the properties from the task that registers the widgets package with the IBM Case Manager server, registers the plug-in for the widgets package with the IBM Content Navigator server, and deploys the EAR file in the widgets package to the web application server, if present. This task is required for the default widgets package that comes with IBM Case Manager. You can also run this task to register your custom widgets packages.

Table 47. Valid task_type and task_name values (continued)

Task type option	Default task display name	Description
`deploysolution`	Deploy Solution	Imports the properties from the task that deploys an IBM Case Manager solution into a production target object store. The properties are stored in the following files: `deploysolution.xml` `deploysolution.`*n*`.xml`. *n* is an integer starting with 2.
`registerboxlistener`	Register the IBM Case Manager Box Event Listener Plug-in	This task registers the plug-in for IBM Content Navigator that listens for case-related Box events when Box collaboration is enabled. This task is required if you want Box events to trigger the creation of cases or work items. Save your changes and run the task to apply your settings.
`registercpeapplets`	Register the IBM Content Platform Engine Applets Support Plug-in	This task registers the plug-in for IBM Content Navigator that contains the Process Designer applet.
`registerexternaldataurl`	Register the External Data Service	This task creates a connection to an external data service, which allows you to use data in a solution from a source other than Content Platform Engine. This task is required only if you are using an external data service in a solution.
`registerprojectarea`	Register Project Area	Imports the properties from the task registers a project area with an IBM Content Navigator desktop, creates the default IBM Case Manager desktops, configures the repositories for the case management design and target object stores, and adds IBM Case Manager features to the desktop. Also, this task configures the Case Operations component queue and configures the project area's isolated region to work with solution workflows. This task is required and must be run for every project area. You must run the Deploy and Register Widgets Package task and the Register the IBM Case Manager Administration Client Plug-in task before you run this task.
`registerservices`	Register the IBM Case Manager Services Plug-in	Imports the properties from the task that registers the plug-in for IBM Content Navigator that contains the IBM Case Manager services that are used by other components. This task is required.

Table 47. Valid task_type and task_name values (continued)

Task type option	Default task display name	Description
`registertargetenv`	Register Target Environment	Imports the properties from the task registers a target environment with an IIBM Content Navigator desktop, creates the default IBM Case Manager desktops, configures the repositories for the case management design and target object stores, and adds IBM Case Manager features to the desktop. Also, this task configures the Case Operations component queue and configures the target environment's isolated region to work with solution workflows. This task is required and must be run for every target environment. You must run the Deploy and Register Widgets Package task and the Register the IBM Case Manager Administration Client Plug-in task before you run this task.
`updatecpeclient`	Update the Content Platform Engine Client Connector files	Imports the properties from the task that downloads the correct version of the Content Platform Engine Client Connector files.
`websphereapplicationserver` or `weblogicapplicationserver`	Application server	Application server settings that are common to all tasks in the profile. These settings are used when you run any of the tasks for the production environment profile. The properties include the application server installation directory, the administrative user name and password, the port number, cell, and other information about the application server. Each profile contains only one of these files, depending on the application server type.
`registericmmonitor`	Register the Case Monitor Widgets Package	This task imports and registers the Case Monitor widgets package with the IBM Case Manager server, registers the plug-in for the widgets package with the IBM Content Navigator server, and creates the Case Monitor desktop. This task is required to enable Case Monitor. Save your changes and run the task to apply your settings. In a cluster environment, you must either use the IBM Content Navigator administration client to manually load the plug-in inside of the extensions package on each node or restart the application server cluster to force all nodes to load the plug-in. Before using Case Monitor, you must create a Case Analyzer store for each case management target object store.

`-sourceTaskName` ***`task_name`***

Specifies the display name for the task that you want to import values from. If you specify the **`sourceTask`** *task_type* parameter, you can omit the **`-sourceTaskName`** *task_type* parameter.

If the display name includes spaces, you must use quotation marks around the display name, as in the following example:

```
-sourceTaskName "Configure LDAP"
```

-target *target_profile*
Specifies the full path to the directory where the target profile is located. The values will be imported into this profile.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Import the properties by specifying the task type.
The following command lists the task mapping for importing the properties for the Configure LDAP task from the builder1 profile into the Configure LDAP task for the develop1 profile:

```
configmgr_cl listImportTargetTasks
 -source
"C:\Program Files\IBM\CaseManagement\configure\profiles\builder1"
 -sourceTask configureldap
 -target
"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1"
```

Import the properties by specifying the display name.
The following command lists the task mapping for importing the task with the display name "Deploy Case Manager Client" from the client2 profile into the "Deploy Case Manager Client" task for the develop1 profile:

```
configmgr_cl listImportTargetTasks
 -source
"C:\Program Files\IBM\CaseManagement\configure\profiles\client2"
 -sourceTaskName "Deploy Case Manager Client"
 -target
"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1"
```

Show the help for the importProps command.
The following command shows the help for the **listImportTargetTasks** command:

```
configmgr_cl listImportTargetTasks -help
```

Related reference:

"**importProps** command" on page 368

listPrincipals command

The **listPrincipals** command lists the users and groups that are assigned to a project area. Users who are not assigned to a project area cannot log in to Case Manager Builder.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl listPrincipals -projectAreaName project_area_name
 -profile myprofile
 [-help]
```

Parameters

-projectAreaName *project_area_name*

The name of the project area. The default project area is named `dev_env_connection_definition`. The name can contain up to 255 characters. If the name includes a space, put the name in double quotation marks, for example, `"Credit Dispute Area"`. The name cannot contain any of the following characters: `\ / : * ? " < > |`

-profile *myprofile*

Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*`/CaseManagement/configure/profiles` directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1"` or `/opt/IBM/CaseManagement/configure/profiles/develop1`.
- The full path to the profile input file, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp"` or `/opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp`.

-help

Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

List the users and groups that area assigned to a project area.

The following command lists the users and groups that are assigned to the project area MyProjectArea for the MyDevelop1 profile:

```
configmgr_cl addPrincipals -projectAreaName MyProjectArea
 -profile MyDevelop1
```

List the users and groups that are assigned to the default project area.

The following command lists the users and groups that are assigned to the default project area for the MyDevelop1 profile:

```
configmgr_cl addPrincipals
 -projectAreaName dev_env_connection_definition
 -profile MyDevelop1
```

Show the help for the addPrincipals command.

The following command shows the help for the **addPrincipals** command:

```
configmgr_cl addPrincipals -help
```

Related reference:

"**addPrincipals** command" on page 316

listSolutions command

The **listSolutions** command lists the solutions that are assigned to a project area.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl listSolutions -projectAreaName project_area_name
 -profile myprofile
 [-help]
```

Parameters

-projectAreaName *project_area_name*

The name of the project area. The default project area is named `dev_env_connection_definition`. The name can contain up to 255 characters. If the name includes a space, put the name in double quotation marks, for example, `"Credit Dispute Area"`. The name cannot contain any of the following characters: `\ / : * ? " < > |`

-profile *myprofile*

Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*`/CaseManagement/configure/profiles` directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1"` or `/opt/IBM/CaseManagement/configure/profiles/develop1`.
- The full path to the profile input file, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp"` or `/opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp`.

-help

Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

List the solutions that area assigned to a project area.

The following command lists the solutions that are assigned to the project area MyProjectArea for the MyDevelop1 profile:

```
configmgr_cl listSolutions -projectAreaName MyProjectArea
 -profile MyDevelop1
```

List the solutions that are assigned to the default project area.

The following command lists the solutions that are assigned to the default project area for the MyDevelop1 profile:

```
configmgr_cl listSolutions
 -projectAreaName dev_env_connection_definition
 -profile MyDevelop1
```

Show the help for the listSolutions command.

The following command shows the help for the **listSolutions** command:

```
configmgr_cl listSolutions -help
```

listTasks command

The **listTasks** command displays a list of the tasks and the task files in the configuration profile.

Syntax

```
configmgr_cl listTasks [-task task_type]  -profile myprofile
 [-help]
```

Parameters

-task *task_type*

Optional. Indicates which task type to list. The following table describes the valid task names, the associated configuration XML file, and a description of the settings affected by the task.

Table 48. task_type values

Option	Configuration file	Description
No value is specified.	A WebSphere Application Server development environment configuration profile can contain the following files: • configbox.xml • configcmos.xml • configibmbpm.xml • configibmcm.xml • configrules.xml • createapps.xml • definedefaultprojectarea.xml • deploycaseapi.xml • deploycaseforms.xml • deploycmbapp.xml • deployibmbpmis.xml • deployregisterextensions.xml • deployregisterwidgets.xml • registeradmin.xml • registerboxlistener.xml • registercpeapplets.xml • registerexternaldataurl.xml • registericmmonitor.xml • registerprojectarea.xml • registerservices.xml • updatecpeclient.xml	If you omit the -task *task_type* parameter, all the configuration tasks and the associated task files for the profile are listed.

Table 48. task_type values (continued)

Option	Configuration file	Description
No value is specified.	An Oracle WebLogic Server development environment configuration profile can contain the following files: • configbox.xml • configcmos.xml • configrules.xml • createapps.xml • definedefaultprojectarea.xml • deploycaseapi.xml • deploycaseforms.xml • deploycmbapp.xml • deployregisterextensions.xml • deployregisterwidgets.xml • registeradmin.xml • registerboxlistener.xml • registercpeapplets.xml • registerexternaldataurl.xml • registericmmonitor.xml • registerprojectarea.xml • registerservices.xml • updatecpeclient.xml	If you omit the `-task task_type` parameter, all the configuration tasks and the associated task files for the profile are listed.
No value is specified.	A WebSphere Application Server production environment configuration profile can contain the following files: • configbox.xml • configcmos.xml • configibmbpm.xml • configibmcm.xml • configrules.xml • createapps.xml • definetargetenv.xml • deploycaseapi.xml • deploycaseforms.xml • deployibmbpmis.xml • deployregisterextensions.xml • deployregisterwidgets.xml • deploysolution.xml • registeradmin.xml • registerboxlistener.xml • registercpeapplets.xml • registerexternaldataurl.xml • registericmmonitor.xml • registerservices.xml • registertargetenv.xml • updatecpeclient.xml	If you omit the `-task task_type` parameter, all the configuration tasks and the associated task files for the profile are listed.

Table 48. task_type values (continued)

Option	Configuration file	Description
No value is specified.	An Oracle WebLogic Server production environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configrules.xml` • `createapps.xml` • `definetargetenv.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `deploysolution.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerservices.xml` • `registertargetenv.xml` • `updatecpeclient.xml`	If you omit the `-task` *`task_type`* parameter, all the configuration tasks and the associated task files for the profile are listed.
`configbox`	`configbox.xml`	This task is required if you want to enable case workers to use Box to collaborate with external users. This task configures the connection to the Box server.
`configcaseloginmodules`	`configcaseloginmodules.xml`	Lists the task that configures the login modules for the Case Manager Builder application. The login modules provide authentication information for the Case Manager Builder application. If you are deploying Case Manager Builder to the same application server where Content Engine is deployed, skip this task.

Table 48. task_type values (continued)

Option	Configuration file	Description
`configcmos`	`configcmos.xml`	Lists the task that configures the design and target object stores. This task installs the IBM Case Manager Add-ons and creates the required events and subscriptions in Content Engine.
`configibmbpm`	`configibmbpm.xml`	Configure IBM Business Process Manager task. This task configures the connection to the IBM Business Process Manager host server. This task is required if you use IBM Business Process Manager as the workflow server for IBM Case Manager.
`configibmcm`	`configibmcm.xml`	Lists the task that configures IBM Content Manager for use with IBM Case Manager.
`configrules`	`configrules.xml`	Lists the task that configures business rules in your solution.

Table 48. task_type values (continued)

Option	Configuration file	Description
`configureldap`	`configureldap.xml` `configureldap.`*n*`.xml` . *n* is an integer starting with 2.	Lists the tasks that configure the directory service provider (LDAP) settings for the Case Manager Builder application. The directory service provider (LDAP) settings define the directory service and the users and groups that uses for authentication. When you generate a second connection definition configuration file in the same profile, it is named `configureldap.2.xml`. The file name increments for each new file that you generate. You cannot change the file name, but you can edit the value in the file for the name of the task.
`createapps`	`createapps.xml`	Lists the task that updates the IBM Case Manager API WAR file and the Case Manager Builder EAR file with system parameters.
`definedefaultprojectarea`	`definedefaultprojectarea.xml`	Lists the task that defines the default project area and the connection definition for the development environment target object store.
`definetargetenv`	`definetargetenv.xml`	Lists the task that defines a target environment for the production environment.

Table 48. task_type values (continued)

Option	Configuration file	Description
`deploycaseapi`	`deploycaseapi.xml`	Lists the task that deploys the IBM Case Manager API application on the web application server. Deploying the IBM Case Manager API application makes the application available for use by the IBM Case Manager application.
`deploycaseforms`	`deploycaseforms.xml`	Lists the task that deploys forms applications.
`deploycmbapp`	`deploycmbapp.xml`	Lists the task that deploys a Case Manager Builder instance on the web application server. Deploying makes the Case Manager Builder application available for use.
`deployibmbpmis`	`deployibmbpmis.xml`	Use with the **`-profileType`** *profile_type* option to generate the file for deploying IBM Business Process Manager. This option generates the following file: `deployibmbpmis.xml`
`deployregisterextensions`	`deployregisterextensions.xml`	This task registers and deploys your extensions package.
`deployregisterwidgets`	`deployregisterwidgets.xml`	Lists the task that registers and deploys a widget package with Case Manager Builder and IBM Content Navigator.

Table 48. task_type values (continued)

Option	Configuration file	Description
`deploysolution`	`deploysolution.xml` `deploysolution.`*n*`.xml`. *n* is an integer starting with 2.	Lists the tasks that deploy an IBM Case Manager solution into a production target object store. You need one configuration file for each production environment target object store that you deploy a solution to. When you generate a second solution deployment configuration file in a profile, it is named `deploysolution.2.xml`. The file name increments for each new file that you generate. You cannot change the file name, but you can edit the value in the file for the name of the task.
`registeradmin`	`registeradmin.xml`	Lists the task that registers the IBM Case Manager administration client with IBM Content Navigator.
`registercpeapplets`	`registercpeapplets.xml`	This task registers the plug-in for IBM Content Navigator that contains the Process Designer applet.
`registerexternaldataurl`	`registerexternaldataurl.xml`	Lists the task that registers a data source other than Content Platform Engine.
`registerprojectarea`	`registerprojectarea.xml`	Lists the task that registers the project area with IBM Content Navigator and configures the Content Platform Engine repositories.

Table 48. task_type values (continued)

Option	Configuration file	Description
registertargetenv	registertargetenv.xml	Lists the task that registers the target environment with IBM Content Navigator and configures the Content Platform Engine repositories.
registerexternaldataurl	registerexternaldataurl.xml	Lists the task that registers an external data source URL with IBM Case Manager.
registerservices	registerservices.xml	This task registers the plug-in for IBM Content Navigator that contains the IBM Case Manager services that are used by other components.
updatecpeclient	updatecpeclient.xml	Lists the task that updates the client connector files for Content Platform Engine.

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

List all the configureldap tasks in a Case Manager Builder profile with multiple configureldap.*n*.xml files.

The following command lists all the configure case login module tasks and the associated configuration XML files in the build profile in the *install_path*/CaseManagement/configure/profiles/develop1 directory:

```
configmgr_cl listTasks -task configureldap -profile develop1
```

A message such as the following example is displayed:

```
Tasks in profile build of the task type configureldap:
Task name: Configure LDAP
        File: configureldap.xml
Task name: Configure the LDAP Settings
        File: configureldap.2.xml
```

Show the help for the listTasks command.

The following command shows the help for the **listTasks** command:

```
configmgr_cl listTasks -help
```

modifyProjectArea command

The **modifyProjectArea** command changes the project area description or connection point.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl modifyProjectArea
 -profile myprofile
 -projectAreaName project_area_name
 -projectAreaDesc project_area_description
 -peConnPt connection_point_name
 [-silent] [-force] [-help]
```

Parameters

-profile *myprofile*

Specifies the development profile that is associated with the project area. The object store and Content Engine properties from the profile are used to create the project area. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-projectAreaName *project_area_name*

The name of the project area. The default project area is named dev_env_connection_definition. The name can contain up to 255 characters. If the name includes a space, put the name in double quotation marks, for example, "Credit Dispute Area". The name cannot contain any of the following characters: \ / : * ? " < > |

-projectAreaDesc *project_area_description*

The description can contain up to 255 characters. If the description includes a space, put the description in double quotation marks, for example, "Solutions for credit card disputes".

-peConnPt *connection_point_name*

The connection point to use with this project area.

-silent

Optional: When you specify the **-silent** parameter, no prompts or

informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Change the project area description.
The following command changes the description for the existing project area CreditDisputeProject for the profile myDevelop1:

```
configmgr_cl modifyProjectArea
 -profile myDevelop1
 -projectAreaName CreditDisputeProject
 -projectAreaDescription "Credit Dispute project area"
  [-silent] [-force]
```

Modify the connection point.
The following command changes the connection point to P8connpoint for the project area named CreditDisputeProject with the profile myDevelop1:

```
configmgr_cl modifyProjectArea
 -profile myDevelop1
 -projectAreaName CreditDisputeProject
 -peConnPt P8connpoint
  [-silent] [-force]
```

Show the help for the modifyProjectArea command.
The following command shows the help for the **modifyProjectArea** command:

```
configmgr_cl modifyProjectArea -help
```

Related reference:

"**defineProjectArea** command" on page 330

moveTask command

The **moveTask** command moves a task to a different position in the list of tasks. The task position determines the order that the tasks are run when you run all the tasks at the same time. You use the **listTasks** command to show the task order.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl moveTask -task task_type | -taskfile task_file_name
-position new_position -profile myprofile [-silent][-force][-help]
```

Parameters

-task *task_type*

Indicates which task to move. This parameter must be included if the **-taskfile** *task_file_name* parameter is omitted. The following table describes the valid task names, the associated configuration XML file, and a description of the settings affected by the task.

Table 49. task_type values

Option	Configuration file	Description
No value is specified.	A WebSphere Application Server development environment configuration profile can contain the following files: • configbox.xml • configcmos.xml • configibmbpm.xml • configibmcm.xml • configrules.xml • createapps.xml • definedefaultprojectarea.xml • deploycaseapi.xml • deploycaseforms.xml • deploycmbapp.xml • deployibmbpmis.xml • deployregisterextensions.xml • deployregisterwidgets.xml • registeradmin.xml • registerboxlistener.xml • registercpeapplets.xml • registerexternaldataurl.xml • registericmmonitor.xml • registerprojectarea.xml • registerservices.xml • updatecpeclient.xml	If you omit the -task *task_type* parameter, all the configuration tasks and the associated task files for the profile are moved.

Table 49. task_type values (continued)

Option	Configuration file	Description
No value is specified.	An Oracle WebLogic Server development environment configuration profile can contain the following files: • configbox.xml • configcmos.xml • configrules.xml • createapps.xml • definedefaultprojectarea.xml • deploycaseapi.xml • deploycaseforms.xml • deploycmbapp.xml • deployregisterextensions.xml • deployregisterwidgets.xml • registeradmin.xml • registerboxlistener.xml • registercpeapplets.xml • registerexternaldataurl.xml • registericmmonitor.xml • registerprojectarea.xml • registerservices.xml • updatecpeclient.xml	If you omit the `-task task_type` parameter, all the configuration tasks and the associated task files for the profile are moved.
No value is specified.	A WebSphere Application Server production environment configuration profile can contain the following files: • configbox.xml • configcmos.xml • configibmbpm.xml • configibmcm.xml • configrules.xml • createapps.xml • definetargetenv.xml • deploycaseapi.xml • deploycaseforms.xml • deployibmbpmis.xml • deployregisterextensions.xml • deployregisterwidgets.xml • deploysolution.xml • registeradmin.xml • registerboxlistener.xml • registercpeapplets.xml • registerexternaldataurl.xml • registericmmonitor.xml • registerservices.xml • registertargetenv.xml • updatecpeclient.xml	If you omit the `-task task_type` parameter, all the configuration tasks and the associated task files for the profile are moved.

Table 49. task_type values (continued)

Option	Configuration file	Description
No value is specified.	An Oracle WebLogic Server production environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configrules.xml` • `createapps.xml` • `definetargetenv.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `deploysolution.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerservices.xml` • `registertargetenv.xml` • `updatecpeclient.xml`	If you omit the `-task` *`task_type`* parameter, all the configuration tasks and the associated task files for the profile are moved.
`configbox`	`configbox.xml`	This task is required if you want to enable case workers to use Box to collaborate with external users. This task configures the connection to the Box server.
`configcaseloginmodules`	`configcaseloginmodules.xml`	Moves the task that configures the login modules for the Case Manager Builder application. The login modules provide authentication information for the Case Manager Builder application. If you are deploying Case Manager Builder to the same application server where Content Engine is deployed, skip this task.

Table 49. task_type values (continued)

Option	Configuration file	Description
`configcmos`	`configcmos.xml`	Moves the task that configures the design and target object stores. This task installs the IBM Case Manager Add-ons and creates the required events and subscriptions in Content Engine.
`configibmbpm`	`configibmbpm.xml`	Moves the task that configures the connection to the IBM Business Process Manager host server. This task is required if you use IBM Business Process Manager as the workflow server for IBM Case Manager.
`configibmcm`	`configibmcm.xml`	Moves the task that configures IBM Content Manager for use with IBM Case Manager.
`configrules`	`configrules.xml`	Moves the task that configures business rules in your solution.

Table 49. task_type values (continued)

Option	Configuration file	Description
`configureldap`	`configureldap.xml` `configureldap.`*n*`.xml` . *n* is an integer starting with 2.	Moves the tasks that configure the directory service provider (LDAP) settings for the Case Manager Builder application. The directory service provider (LDAP) settings define the directory service and the users and groups that uses for authentication. When you generate a second connection definition configuration file in the same profile, it is named `configureldap.2.xml`. The file name increments for each new file that you generate. You cannot change the file name, but you can edit the value in the file for the name of the task.
`createapps`	`createapps.xml`	Moves the task that updates the IBM Case Manager API WAR file and the Case Manager Builder EAR file with system parameters.
`definedefaultprojectarea`	`definedefaultprojectarea.xml`	Moves the task that defines the default project area and the connection definition for the development environment target object store.
`definetargetenv`	`definetargetenv.xml`	Moves the task that defines a target environment for the production environment.

Table 49. task_type values (continued)

Option	Configuration file	Description
`deploycaseapi`	`deploycaseapi.xml`	Lists the task that deploys the IBM Case Manager API application on the web application server. Deploying the IBM Case Manager API application makes the application available for use by the IBM Case Manager application.
`deploycaseforms`	`deploycaseforms.xml`	Moves the task that deploys forms applications.
`deploycmbapp`	`deploycmbapp.xml`	Moves the task that deploys a Case Manager Builder instance on the web application server. Deploying makes the Case Manager Builder application available for use.
`deployibmbpmis`	`deployibmbpmis.xml`	Use with the **`-profileType`** *profile_type* option to generate the file for deploying IBM Business Process Manager. This option generates the following file: `deployibmbpmis.xml`
`deployregisterextensions`	`deployregisterextensions.xml`	This task registers and deploys your extensions package.
`deployregisterwidgets`	`deployregisterwidgets.xml`	Moves the task that registers and deploys a widget package with Case Manager Builder and IBM Content Navigator.

Table 49. task_type values (continued)

Option	Configuration file	Description
`deploysolution`	`deploysolution.xml` `deploysolution.`*n*`.xml`. *n* is an integer starting with 2.	Moves the tasks that deploy an IBM Case Manager solution into a production target object store. You need one configuration file for each production environment target object store that you deploy a solution to. When you generate a second solution deployment configuration file in a profile, it is named `deploysolution.2.xml`. The file name increments for each new file that you generate. You cannot change the file name, but you can edit the value in the file for the name of the task.
`registeradmin`	`registeradmin.xml`	Moves the task that registers the IBM Case Manager administration client with IBM Content Navigator.
`registercpeapplets`	`registercpeapplets.xml`	This task registers the plug-in for IBM Content Navigator that contains the Process Designer applet.
`registerexternaldataurl`	`registerexternaldataurl.xml`	Moves the task that registers a data source other than Content Platform Engine.
`registerprojectarea`	`registerprojectarea.xml`	Moves the task that registers the project area with IBM Content Navigator and configures the Content Platform Engine repositories.

Table 49. task_type values (continued)

Option	Configuration file	Description
`registertargetenv`	`registertargetenv.xml`	Moves the task that registers the target environment with IBM Content Navigator and configures the Content Platform Engine repositories.
`registerexternaldataurl`	`registerexternaldataurl.xml`	Moves the task that registers an external data source URL with IBM Case Manager.
`registerservices`	`registerservices.xml`	This task registers the plug-in for IBM Content Navigator that contains the IBM Case Manager services that are used by other components.
`updatecpeclient`	`updatecpeclient.xml`	Moves the task that updates the client connector files for Content Platform Engine.

-taskfile *task_file_name*
Specifies the *configuration*`.xml file` to use.

If only one task file exists for the *task_type*, the **-taskfile** *task_file_name* parameter is optional.

If more than one task file for the *task_type* exists, you must include the **-taskfile** *task_file_name* parameter. The *task_file* value is case sensitive if your operating system is case sensitive for file names.

-position *new_position*

Specifies the new position in the list for the item. You can run the **listTasks** command to view the list of tasks in the profile and their position before you run the **moveTask** command.

Remember: Task order is critical when you use the **execute** command to run all tasks at one time. Some tasks must be run in a specific order. If you must move a task, ensure that you keep the required order for tasks that have a prerequisite.

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*`/CaseManagement/configure/profiles` directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1"` or `/opt/IBM/CaseManagement/configure/profiles/develop1`.

- The full path to the profile input file, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp"` or `/opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp`.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Move the task for the `configureldap.2.xml` file in a profile with more than one `configureldap` task. By default, the `configureldap.xml` file is in position 2.
The following command moves the task for the `configureldap.2.xml` file for the build profile in the *install_path*`/CaseManagement/configure/profiles/develop1` directory to position 2:

```
configmgr_cl moveTask -taskfile configureldap.2.xml -position 2
-profile develop1
```

Show the help for the moveTask command.
The following command shows the help for the **moveTask** command:

```
configmgr_cl moveTask -help
```

removePrincipals command

The **removePrincipals** command removes a user or group from a project area. Users who are not assigned to a project area cannot log in to Case Manager Builder.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl removePrincipals -projectAreaName project_area_name
 -profile myprofile
 [-users user_name] [-groups group_name]
 [-silent] [-force] [-help]
```

Parameters

-projectAreaName *project_area_name*
Specifies the name of the project area. The default project area is named dev_env_connection_definition.

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-users *user_name*

Specifies the short name or display name of the user to remove. A user can belong to the default project area and one other project area.

You can remove multiple users at one time by adding additional -users *user_name* entries on the same command.

You can omit this option if you are removing only groups.

-groups *group_name*

Specifies the short name or display name of the group that you want to remove. Groups can belong to the default project area only.

You can remove multiple groups at one time by adding additional -groups *group_name* entries on the same command.

You can omit this option if you are removing only users.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Remove a single user.
The following command removes the user MariaG from the project area MyProjectArea in the MyDevelop1 profile:

```
configmgr_cl removePrincipals -projectAreaName MyProjectArea
 -profile MyDevelop1
 -users MariaG
```

Remove a group from the default project area.

The following command removes the group CaseDevelopers from the default project area in the MyDevelop1 profile:

```
configmgr_cl removePrincipals
 -projectAreaName dev_env_connection_definition
 -profile MyDevelop1
 -groups CaseDevelopers
```

Remove several users from a project area.

The following command removes the users MariaG, BarneyF, and JoseP from the project area MyProjectArea in the MyDevelop1 profile:

```
configmgr_cl removePrincipals -projectAreaName MyProjectArea
 -profile MyDevelop1
 -users MariaG -users BarneyF -users JoseP
```

Remove several users and a single group from the default project area.

The following command removes the users MariaG, BarneyF, and JoseP and the group CaseDevelopers from the default project area in the MyDevelop1 profile:

```
configmgr_cl removePrincipals -projectAreaName
  dev_env_connection_definition
 -profile MyDevelop1
 -users MariaG -users BarneyF -users JoseP
 -groups CaseDevelopers
```

Show the help for the removePrincipals command.

The following command shows the help for the **removePrincipals** command:

```
configmgr_cl removePrincipals -help
```

Related reference:

"**addPrincipals** command" on page 316

removeSolutions command

The **removeSolutions** command removes a solution from a project area. When you remove a solution from a project area, the solution is automatically added to the default project area.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl removeSolutions -projectAreaName project_area_name
 -profile myprofile
 -solutions solution_name [-solutions solution_name_n]
 [-silent] [-force] [-help]
```

Parameters

-projectAreaName *project_area_name*

Specifies the name of the project area to remove the solutions from. The default project area is named dev_env_connection_definition.

-profile *myprofile*

Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-solutions *solution_name*
Specifies the solution name. You can enter multiple -solutions *solution_name* options on the same command line.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Remove a solution.
The following command removes the Solution1 solution from the CreditDisputeArea project area for the development environment that was configured with the myDevelop1 profile:

```
configmgr_cl removeSolutions -projectAreaName CreditDisputeArea
 -profile myDevelop1
 -solutions Solution1
 [-silent] [-force]
```

Remove two solutions.
The following command removes the Solution1 solution and the Solution2 solution from the CreditDisputeArea project area for the development environment that was configured with the myDevelop1 profile:

```
configmgr_cl removeSolutions -projectAreaName CreditDisputeArea
 -profile myDevelop1
 -solutions Solution1  -solutions Solution2
 [-silent] [-force]
```

Show the help for the removeSolutions command.
The following command shows the help for the **removeSolutions** command:

```
configmgr_cl removeSolutions -help
```

Related reference:

"**addSolutions** command" on page 318

removeTask command

The **removeTask** command removes the specified task from the configuration profile. When you remove the task, the configuration XML file is deleted from the profile directory. You cannot recover a task file that has been deleted from a profile.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl removetask -task task_type | -taskfile task_file_name
 -profile myprofile [-silent][-force][-help]
```

Parameters

-task *task_type*

Indicates which task to remove. This parameter must be included if the **-taskfile** *task_file_name* parameter is omitted. The following table describes the valid task names, the associated configuration XML file, and a description of the settings affected by the task.

Table 50. task_type values

Option	Configuration file	Description
No value is specified.	A WebSphere Application Server development environment configuration profile can contain the following files: • configbox.xml • configcmos.xml • configibmbpm.xml • configibmcm.xml • configrules.xml • createapps.xml • definedefaultprojectarea.xml • deploycaseapi.xml • deploycaseforms.xml • deploycmbapp.xml • deployibmbpmis.xml • deployregisterextensions.xml • deployregisterwidgets.xml • registeradmin.xml • registerboxlistener.xml • registercpeapplets.xml • registerexternaldataurl.xml • registericmmonitor.xml • registerprojectarea.xml • registerservices.xml • updatecpeclient.xml	If you omit the -task *task_type* parameter, all the configuration tasks and the associated task files for the profile are removed.

Table 50. task_type values (continued)

Option	Configuration file	Description
No value is specified.	An Oracle WebLogic Server development environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configrules.xml` • `createapps.xml` • `definedefaultprojectarea.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deploycmbapp.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registercpeapplets.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerprojectarea.xml` • `registerservices.xml` • `updatecpeclient.xml`	If you omit the `-task` *`task_type`* parameter, all the configuration tasks and the associated task files for the profile are removed.
No value is specified.	A WebSphere Application Server production environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configibmbpm.xml` • `configibmcm.xml` • `configrules.xml` • `createapps.xml` • `definetargetenv.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deployibmbpmis.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `deploysolution.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registercpeapplets.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerservices.xml` • `registertargetenv.xml` • `updatecpeclient.xml`	If you omit the `-task` *`task_type`* parameter, all the configuration tasks and the associated task files for the profile are removed.

Table 50. task_type values (continued)

Option	Configuration file	Description
No value is specified.	An Oracle WebLogic Server production environment configuration profile can contain the following files: • `configbox.xml` • `configcmos.xml` • `configrules.xml` • `createapps.xml` • `definetargetenv.xml` • `deploycaseapi.xml` • `deploycaseforms.xml` • `deployregisterextensions.xml` • `deployregisterwidgets.xml` • `deploysolution.xml` • `registeradmin.xml` • `registerboxlistener.xml` • `registerexternaldataurl.xml` • `registericmmonitor.xml` • `registerservices.xml` • `registertargetenv.xml` • `updatecpeclient.xml`	If you omit the `-task` *`task_type`* parameter, all the configuration tasks and the associated task files for the profile are removed.
`configbox`	`configbox.xml`	This task is required if you want to enable case workers to use Box to collaborate with external users. This task configures the connection to the Box server.
`configcaseloginmodules`	`configcaseloginmodules.xml`	Removes the task that configures the login modules for the Case Manager Builder application. The login modules provide authentication information for the Case Manager Builder application. If you are deploying Case Manager Builder to the same application server where Content Engine is deployed, skip this task.

Table 50. task_type values (continued)

Option	Configuration file	Description
`configcmos`	`configcmos.xml`	Removes the task that configures the design and target object stores. This task installs the IBM Case Manager Add-ons and creates the required events and subscriptions in Content Engine.
`configibmbpm`	`configibmbpm.xml`	Configure IBM Business Process Manager task. This task configures the connection to the IBM Business Process Manager host server. This task is required if you use IBM Business Process Manager as the workflow server for IBM Case Manager.
`configibmcm`	`configibmcm.xml`	Removes the task that configures IBM Content Manager for use with IBM Case Manager.
`configrules`	`configrules.xml`	Removes the task that configures business rules in your solution.

Table 50. task_type values (continued)

Option	Configuration file	Description
`configureldap`	`configureldap.xml` `configureldap.`*n*`.xml` . *n* is an integer starting with 2.	Removes the tasks that configure the directory service provider (LDAP) settings for the Case Manager Builder application. The directory service provider (LDAP) settings define the directory service and the users and groups that uses for authentication. When you generate a second connection definition configuration file in the same profile, it is named `configureldap.2.xml`. The file name increments for each new file that you generate. You cannot change the file name, but you can edit the value in the file for the name of the task.
`createapps`	`createapps.xml`	Removes the task that updates the IBM Case Manager API WAR file and the Case Manager Builder EAR file with system parameters.
`definedefaultprojectarea`	`definedefaultprojectarea.xml`	Removes the task that defines the default project area and the connection definition for the development environment target object store.
`definetargetenv`	`definetargetenv.xml`	Removes the task that defines a target environment for the production environment.

Table 50. task_type values (continued)

Option	Configuration file	Description
`deploycaseapi`	`deploycaseapi.xml`	Removes the task that deploys the IBM Case Manager API application on the web application server. Deploying the IBM Case Manager API application makes the application available for use by the IBM Case Manager application.
`deploycaseforms`	`deploycaseforms.xml`	Removes the task that deploys forms applications.
`deploycmbapp`	`deploycmbapp.xml`	Removes the task that deploys a Case Manager Builder instance on the web application server. Deploying makes the Case Manager Builder application available for use.
`deployibmbpmis`	`deployibmbpmis.xml`	Use with the **`-profileType`** *profile_type* option to generate the file for deploying IBM Business Process Manager. This option generates the following file: `deployibmbpmis.xml`
`deployregisterextensions`	`deployregisterextensions.xml`	This task registers and deploys your extensions package.
`deployregisterwidgets`	`deployregisterwidgets.xml`	Removes the task that registers and deploys a widget package with Case Manager Builder and IBM Content Navigator.

Table 50. task_type values (continued)

Option	Configuration file	Description
`deploysolution`	`deploysolution.xml` `deploysolution.`*n*`.xml`. *n* is an integer starting with 2.	Removes the tasks that deploy an IBM Case Manager solution into a production target object store. You need one configuration file for each production environment target object store that you deploy a solution to. When you generate a second solution deployment configuration file in a profile, it is named `deploysolution.2.xml`. The file name increments for each new file that you generate. You cannot change the file name, but you can edit the value in the file for the name of the task.
`registeradmin`	`registeradmin.xml`	Removes the task that registers the IBM Case Manager administration client with IBM Content Navigator.
`registercpeapplets`	`registercpeapplets.xml`	This task registers the plug-in for IBM Content Navigator that contains the Process Designer applet.
`registerexternaldataurl`	`registerexternaldataurl.xml`	Removes the task that registers a data source other than Content Platform Engine.
`registerprojectarea`	`registerprojectarea.xml`	Removes the task that registers the project area with IBM Content Navigator and configures the Content Platform Engine repositories.

Table 50. task_type values (continued)

Option	Configuration file	Description
`registertargetenv`	`registertargetenv.xml`	Removes the task that registers the target environment with IBM Content Navigator and configures the Content Platform Engine repositories.
`registerexternaldataurl`	`registerexternaldataurl.xml`	Removes the task that registers an external data source URL with IBM Case Manager.
`registerservices`	`registerservices.xml`	This task registers the plug-in for IBM Content Navigator that contains the IBM Case Manager services that are used by other components.
`updatecpeclient`	`updatecpeclient.xml`	Removes the task that updates the client connector files for Content Platform Engine.

-taskfile *task_file_name*
Specifies the *configuration*`.xml file` to use.

If only one task file exists for the *task_type*, the **-taskfile** *task_file_name* parameter is optional.

If more than one task file for the *task_type* exists, you must include the **-taskfile** *task_file_name* parameter. The *task_file* value is case sensitive if your operating system is case sensitive for file names.

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*`/CaseManagement/configure/profiles` directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1"` or `/opt/IBM/CaseManagement/configure/profiles/develop1`.
- The full path to the profile input file, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp"` or `/opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp`.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Remove the configureldap task from a profile with only one configureldap task.
The following command removes the configureldap task and the configureldap.xml file from the profile named develop1.

```
configmgr_cl removeTask -task configureldap -profile develop1
```

Remove the configureldap task from a profile with several configureldap tasks.
The following command removes the configureldap task and the configureldap.2.xml file from the profile named develop2:

```
configmgr_cl removeTask -taskfile configureldap.2.xml
 -profile develop2
```

Remove the configureldap task from a profile with several configureldap tasks by using a full path to the profile directory.
The following command removes the configureldap task and the configureldap.2.xml file from the profile named develop2 that is in the /temp/myprofiles/develop2 directory:

```
configmgr_cl removeTask -taskfile configureldap.2.xml
 -profile  /temp/myprofiles/develop2
```

Show the help for the removeTask command.
The following command shows the help for the **removeTask** command:

```
configmgr_cl removeTask -help
```

storePasswords command

The **storePasswords** command prompts for passwords that are blank in a profile and stores the encrypted passwords in the file. Storing encrypted passwords might not be FIPS 140-2 compliant, and you can cancel the command after the prompt about compliance.

Syntax

You can run the command for a single task or for all tasks in the profile. If a password entry in a configuration XML file is not blank, the following message is displayed.

```
There are no missing passwords to store.
```

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl storePasswords [-task task_type | -taskfile task_file_name]
 -profile myprofile [-help]
```

Parameters

-task *task_type*

The **-task** *task_type* parameter specifies a specific task to encrypt the passwords for. You can omit the **-task** *task_type* parameter if you want to store passwords for all the tasks or if you specify the **-taskfile** *task_file_name* parameter.

If you omit the **-task** *task_type* parameter and the **-taskfile** *task_file_name* parameter, you are prompted to enter the passwords for each configuration XML file in the profile. Each password is encrypted before it is added to the XML file.

Table 51. Passwords and files

Password description	Property name and XML file name
Application server administrator password	ApplicationServerAdminPassword property in the `websphereapplicationserver.xml` file or the `weblogicapplicationserver.xml` file.
IBM Content Navigator administrator password	NexusPassword property in the `contentnavigatorserver.xml` file
Content Platform Engine domain user password	CEPassword property in the `contentengineserver.xml` file
Directory service bind user password	LDAPBindPassword property in the `configureldap.xml` file
Case operations password	CaseOperationsPassword property in the `registerprojectarea.xml` file (development environment) or `registertargetenv.xml` file (production environment)
LTPA key password	LTPAKeyPassword property in the `importltpakey.xml` file

When you specify a specific task for the **storePasswords** command, encrypted passwords are added to the task file, the `websphereapplicationserver.xml` or `weblogicapplicationserver.xml` file, the `contentnavigatorserver.xml` file, and the `contentengineserver.xml` file. The following table describes the valid *task_type* and *task_file_name* values, the password property names, and the task configuration XML file names that are affected by the task options.

Table 52. Valid task_type and task_file_name values

task_type **values**	*task_file_name* **values**	**Description**
No value is specified.	No value is specified.	Encrypts the passwords for all the tasks in the profile, as listed in Table 51.
`configbox`	`configbox.xml`	Encrypts the password configuring the Box host properties.
`configibmbpm`	`configibmbpm.xml`	Encrypts the password configuring the IBM Business Process Manager host properties.
`configibmcm`	`configibmcm.xml`	Encrypts the password configuring the IBM Content Manager host properties.
`configrules`	`configrules.xml`	Lists the task that configures business rules in your solution.

Table 52. Valid task_type and task_file_name values (continued)

task_type **values**	*task_file_name* **values**	**Description**
`registerprojectarea`	`registerprojectarea.xml`	Encrypts the case operations user password that is stored in **`CaseOperationsPassword`** property in the `registerprojectarea.xml` file and the IBM Content Navigator administrator password that is stored in the NexusPassword property in the `contentnavigatorserver.xml` file.
`registertargetenv`	`registertargetenv.xml`	Encrypts the case operations user password that is stored in **`CaseOperationsPassword`** property in the `registertargetenv.xml` file and the IBM Content Navigator administrator password that is stored in the NexusPassword property in the `contentnavigatorserver.xml` file.

`-taskfile` ***`task_file_name`***

Specifies the configuration XML file to encrypt the passwords for. You can omit the **`-taskfile`** *task_file_name* parameter if you want to store passwords for all the tasks or if you specify the **`-task`** *task_type* parameter.

If you omit the **`-task`** *task_type* parameter and the **`-taskfile`** *task_file_name* parameter, you are prompted to enter the passwords for each configuration XML file in the profile. Each password is encrypted before it is added to the XML file. The passwords that you enter depend on the type of profile, which is described in Table 51 on page 420.

See Table 52 on page 420 for the valid *task_file_name* values and passwords.

`-profile` ***`myprofile`***

Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *`install_path`*`/CaseManagement/configure/profiles` directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1"` or `/opt/IBM/CaseManagement/configure/profiles/develop1`.
- The full path to the profile input file, such as `"C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp"` or `/opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp`.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Encrypt and save all passwords for a profile.

The following command encrypts and saves passwords for any blank entries in the profile named develop1:

```
configmgr_cl storePasswords -profile develop1
```

Encrypt and save the passwords for the `deploycmbapp.xml` file.

The following command encrypts and saves passwords for any blank entries in the `deploycmbapp.xml` file from the profile named develop2:

```
configmgr_cl storePasswords -taskfile deploycmbapp.xml
 -profile develop2
```

Show the help for the storePasswords command.

The following command shows the help for the **storePasswords** command:

```
configmgr_cl storePasswords -help
```

test command

The **test** command runs the test feature for a task or a profile environment. Some tasks do not have a test function.

Syntax

The following syntax includes line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

```
configmgr_cl test -task task_type | -taskfile task_file_name
 -profile myprofile [-silent][-force][-help]
```

Parameters

`-task` *`task_type`*

Indicates which task to test. This parameter must be included if the **`-taskfile`** *task_file_name* parameter is omitted. The following table describes the valid task names, the associated configuration XML file, and a description of the test performed by the task.

Table 53. task_type values

Option	Configuration file	Description
`configibmbpm`	`configibmbpm.xml`	Tests the connection between the configuration tool, the IBM Business Process Manager host server, and the Content Platform Engine server.
`configibmcm`	`configibmcm.xml`	Tests the connection between the configuration tool, the IBM Content Manager host server, and the Content Platform Engine server.
`deployibmbpmis`	`deployibmbpmis.xml`	Tests the connection between the configuration tool and the Content Platform Engine server.
`deploysolution`	`deploysolution.xml` `deploysolution.`*`n`*`.xml`. *n* is an integer starting with 2.	Opens the role assignment page for you to assign LDAP users to the roles for this solution. You must run the `configmgr_cl execute -taskfile deploysolution.`*`n`* `-profile` *`myprofile`* before you assign roles. You can also assign users later in Case Manager Client.
`registeradmin`	`registeradmin.xml`	Test the connection between the configuration tool and the IBM Content Navigator server and verifies the ID for the selected plug-in.

Table 53. task_type values (continued)

Option	Configuration file	Description
registercpeapplets	registercpeapplets.xml	This task registers the plug-in for IBM Content Navigator that contains the Process Designer applet.
registerprojectarea	registerprojectarea.xml	Test the connection between the configuration tool and the IBM Content Navigator server and verifies the Case Operations user credentials.
registerservices	registerservices.xml	Test the connection between the configuration tool and the IBM Content Navigator server and verifies the ID for the selected plug-in.
registertargetenv	registertargetenv.xml	Test the connection between the configuration tool and the IBM Content Navigator server and verifies the Case Operations user credentials.

-taskfile *task_file_name*
Specifies the *configuration*.xml file to use.

If only one task file exists for the *task_type*, the **-taskfile** *task_file_name* parameter is optional.

If more than one task file for the *task_type* exists, you must include the **-taskfile** *task_file_name* parameter. The *task_file* value is case sensitive if your operating system is case sensitive for file names.

-profile *myprofile*
Specifies the profile to use. The *myprofile* value can be one of the following items:

- The name of the profile, such as develop1. The profile is located in the *install_path*/CaseManagement/configure/profiles directory. *install_path* is the location where IBM Case Manager is installed.
- The full path to the profile directory, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1" or /opt/IBM/CaseManagement/configure/profiles/develop1.
- The full path to the profile input file, such as "C:\Program Files\IBM\CaseManagement\configure\profiles\develop1\develop1.cfgp" or /opt/IBM/CaseManagement/configure/profiles/develop1/develop1.cfgp.

-silent
Optional: When you specify the **-silent** parameter, no prompts or informational messages are shown in the console, but the errors are written to the log. Failure messages and validation error messages are shown as needed, such as messages about missing passwords or invalid port numbers. If you run the **execute** command to run all the tasks in a profile and you specify the **-silent** parameter, you must also specify the **-force** parameter.

-force
Optional and applies only when the **-silent** parameter is used. When you specify the **-force** parameter, the task is run without pausing for required responses to validation error messages, such as messages about missing passwords or invalid port numbers.

-help
Optional: Shows a brief message on the command syntax instead of running the command.

Sample commands

The following examples include line breaks to format the command for reading. Enter the command and options on a single line without any line breaks.

Test the deploysolution task from a profile with only one deploysolution task.
The following command tests the deploysolution task and the deploysolution.xml file from the profile named deploy_one:

```
configmgr_cl test -task deploysolution -profile deploy_one
```

Test the deploysolution task from a profile with several deploysolution tasks.
The following command tests the deploysolution task and the deploysolution.2.xml file from the profile named deploy_many:

```
configmgr_cl test -taskfile deploysolution.2.xml
 -profile deploy_many
```

Test the deploysolution task from a profile with several deploysolution tasks by using an absolute path to the profile directory.
The following command tests the deploysolution task and the deploysolution.2.xml file from the profile named deploy_many that is in the c:\temp\myprofiles\deploy_many directory:

```
configmgr_cl test -taskfile deploysolution.2.xml
-profile  c:\temp\myprofiles\deploy_many
```

Show the help for the test command.
The following command shows the help for the **test** command:

```
configmgr_cl test -help
```

Notices

This information was developed for products and services that are offered in the USA.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those

websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
IBM Director of Licensing
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample

programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

Portions of this code are derived from IBM Corp. Sample Programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these

publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use cookies that collect each user’s user name for purposes of session management, authentication, and enhanced user usability. These cookies cannot be disabled.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at www.ibm.com/privacy and IBM’s Online Privacy Statement at www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at www.ibm.com/software/info/product-privacy.

Index

E

F

G

I

J

K

L

M

O

P

Q

R

S

T

U

V

W

Product Number: 5725-A15

SC19-3683-07