IBM Case Manager 5.2

Security Model: Considerations and Best Practices

Steven Hsieh, Johnson Liu

Special Thanks to Bob Jackson

Abstract

IBM Case Manager 5.2 introduced significant improvements to facilitate how case security is managed. Security can now be configured from the IBM Case Manager system by using the case management solution oriented view.

A major portion of the security prior to 5.2 was done in the Content Engine using Administration Console for Content Engine or Filenet Enterprise Management. The Process Engine security for Case Tasks was configured using Process Configuration Console. IBM Case Foundation security provides many options that require the Case Manager solution design team and administrators to understand the IBM Case Foundation system well enough to communicate and implement their business requirements.

It is still possible for the IBM Case Foundation administrator to directly manage the security settings by configuring the solution elements in the target object or workflow system. However, those security settings cannot be easily captured in a portable way and are difficult to manage and keep track of across environments. When a solution is transferred through its lifecycle or from environment to environment, for example from development to test, the settings are lost.

The IBM Case Manager security wizards provide the ability to apply case management security settings on a solution basis. The settings are tracked in configuration file that are based on configurable privilege definition. The privilege definition aggregate the various content- and workflow-related permissions and organize the permissions into logical settings appropriate for a case management environment.

Security manifests can be created for the various environments. Alternatively, a single manifest can be used throughout the solution lifecycle where the LDAP configurations are consistent. When ready, the security manifest can then be applied to the case management system.

The security manifests are portable. They are associated with the solution and packaged for transfer using the IBM Case Manager administration client (http://<hostname>:9080/navigator/?desktop=icmadmin). From there, the security configurations can be exported and transferred from environment to environment.

This article introduces the basics of the security configuration, as well as best practices and additional business scenarios. It is not intended as an exhaustive source.

Revision 1.0

Contents

Security Considerations

IBM Case Manager V5.2

Planning and Preparation

Solution Design and Migration Lifecycle

Organizations often define formal and informal development lifecycles that range from simple to complex. For our purposes, we will use a four stage migration: **Development → Integration Test (IT) → User Acceptance Test (UAT)-Preproduction → Production**. From solution design to configuring the case security model, there are various stages of the development lifecycle involved. As shown in Figure 1, the solution development vs. security configuration are usually started from the various lifecycle stages.
On the left side of the following diagram, the Development environment and IT environment have a development profile. On the right side, the UAT/Preproduction environment and Production environment have a production profile. However, more and more customers are migrating their IT environment to a production profile model to start their security configuration and testing at an earlier stage of the lifecycle. That is why you see an overlap in the diagram.
The bubble labeled Source Control in the diagram shows how some customers are now further controlling the solution package by using source control. Customers can import and deploy the same solution package across the different stages of the environments. If they want to make changes, they must go back to the Development environment to ensure they have a consistent solution package and have version control on the solution package.
In UAT/Preproduction environment, we begin to build the security configuration. We can export this configuration, then import or apply it into production. However, we recommend to start building the security configuration in the IT environment.

Further, the security configuration can also be checked into source control to guarantee the same configuration package is used when migrating across environments.

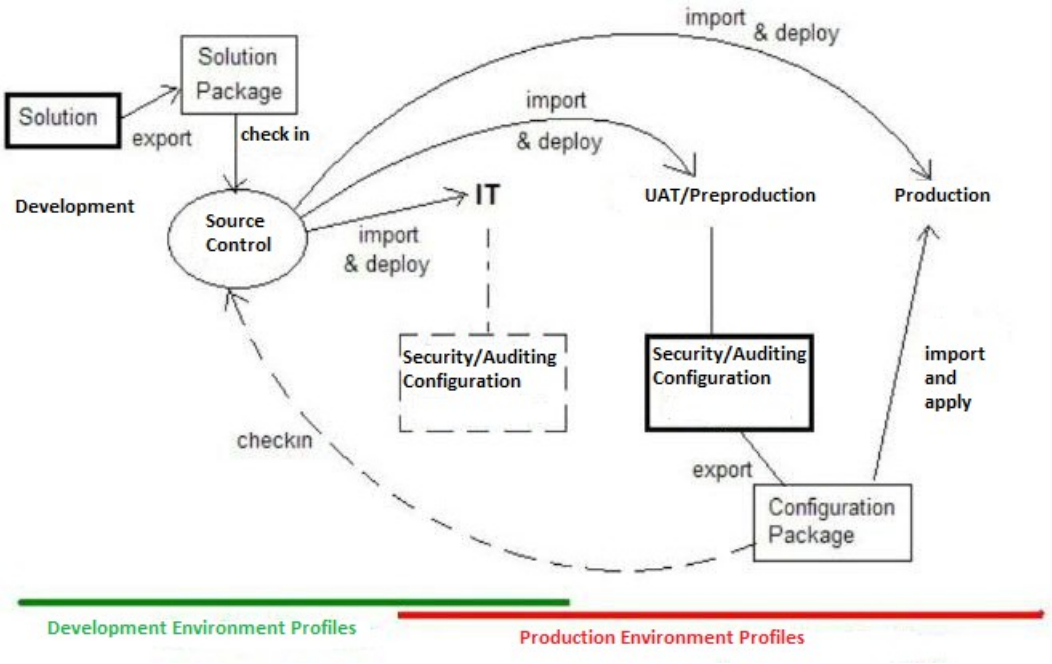


Figure 1 Lifecycle Relationship to Security Configuration

Prior Planning Prevents Problems: Case Security Model

In addition to business scenarios for a solution, it is also important for the solution developer to discover and understand the end user's security requirements within the overall business context. For example, when designing a commercial lending application, all the involved roles and their corresponding security rights must be properly identified and configured. Otherwise, a user might not be able to effectively interact with the solution because they do not have correct access rights to see the case documents or to update the case information.

Various parts of an organization will produce the security requirements of a solution. The stakeholders include:

- Business users who use the solution
- Corporate security professionals who set security strategy
- Business analysts and solution designers who design and configure the solution
- System administrators who implement the security strategy

Early in the design lifecycle, the various stakeholders must agree on the solution security strategy so that the resulting solution includes the elements to support the business operation properly. The strategy needs to take into account the various end user roles along with the business and legal requirements that are necessary to provide access and regulatory compliance. Security aspects of a solution are best planned while the solution is still under design and development to avoid redesign and late-found security issues. When deciding on the business model as well as security requirements for a given solution, basic questions should be in the forefront:

- What problem is being solved by the solution?

- Who participates in driving the case to resolution and what are their roles?
- How can each role collaborate on their work?
- What authorizations are needed to allow a given role to complete their activities?

These requirements will also feed into test plan and scenario coverages. Along with other design and architectural aspects of the project plan, the project manager must also include sufficient time for security testing to ensure overall business solution delivery quality.

Security Planning

The security planning for Case Manager and the underlying Case Foundation platforms involves two aspects: authentication and authorization. Authentication deals with verifying that the user who is taking the action is who they claim to be. Normally, this is done at login with the user password.
Authorization deals with determining what that user is allowed to do after he or she has authenticated to the system. This article only deals with authorizations applied to users after they have completed authentication. Authorization is also commonly referred to as access or user rights.
Just as there are multiple stakeholders in determining the authorizations for a given solution, the determining and implementing the settings can involved more than one person. As shown in the following table, an organization might have one or more people implementing the security for a given solution. When the security requirements are well documented, each of the implementors knows what he or she needs to do so that the solution is properly secured.

Implementor	Description
LDAP Administration	Configures the LDAP server by creating, updating, and deleting users and groups used by the solution.
IBM Case Foundation Administrator	Manages the assignment of access rights to users in the underlying IBM Case Foundation system.
IBM Case Manager Administrator	Implements security for the case management system.
Solution Administrator	Administers one or more case management solutions.
Solution Designer	Works directly on the solution design.

The Value of LDAP Groups

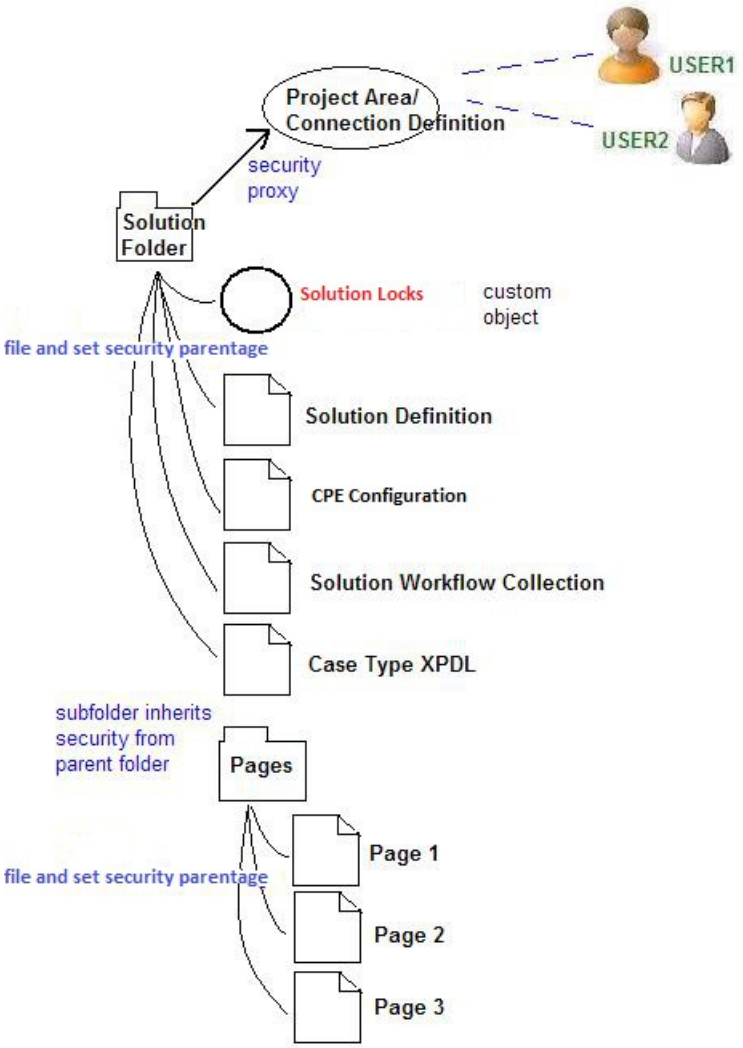
When planning the security for a given solution, LDAP groups aggregate users into manageable groupings to simplify the assignment of authorization for various aspects of the solution components. While users can be directly assigned to the roles to manage security rights, using LDAP groups allows the solution designer and administrator to manage security more logically through functional roles and then indirectly controls user's access rights by adjusting LDAP group memberships of a user.

A master group is a LDAP group that contains groups, users, or both to allow for large-scale authorization. The system provides a special pseudo group called #AUTHENTICATED-USERS. After a user is authenticated to the system, that user automatically belongs to this master group. IBM Case Manager recommends that organizations create additional master groups to facilitate authorization management. Examples of such groups are Case Administrators and Case Users, which in turn would contains real enterprise organizational business LDAP groups such as IT Administrators, Loan Officers, Finance, Underwriters, and so on. Using these master groups allows the system administrator and the case administrator to provide access rights management without forcing them to manage individual users.

Design Object Store Security

The IT/IBM Case Manager Solution Administrator has control over the design object store and the staging object store. The design object store in development environment is treated just like a source control system. Only the authorized business analyst groups and users that are assigned to a project area have authoring rights to the corresponding solutions within that project area.

The solution security is dynamically reflected from the groups and users that are assigned to project area down to the solution folder and the additional artifacts within the solution as shown in the following diagram:



Target Environment Security

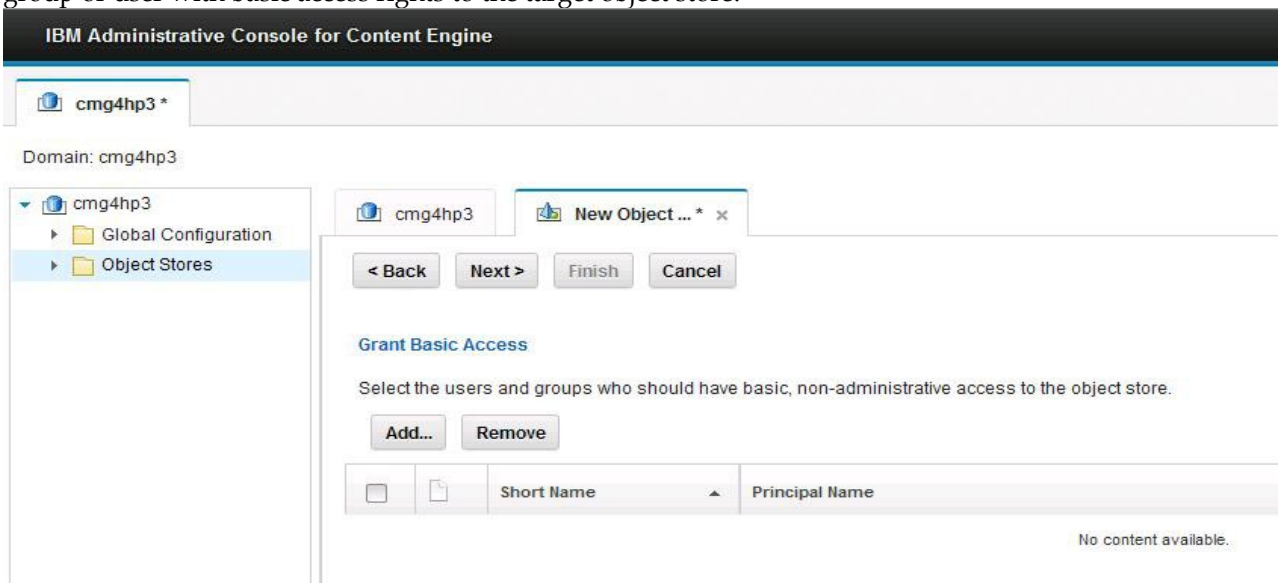
Regardless of the number of tiers in the design lifecycle, each organization has one or more target environments. These environments might rely on the same or different LDAP server configurations. Further, the authorizations for a given solution will evolve as the solution is passed from environment to environment.

The security manifests that the solution administrators configures must reflect the differing authorizations that are required at each stage. This security is analogous to building a government office building where construction workers have free access to the office building until it is completed. After construction is completed, the doors are locked, the security is instrumented based on job functionality and required clearance, and access privileges are given only to the security guards, government employees, project contractors, cleaning crew, and so on accordingly.

At the development level, the solution developers require fairly unrestricted access to design the solution elements and to deploy the solution to try out the solution in the runtime environment. This access requirement might continue through various testing phases. At some point in the development lifecycle, these authorizations are removed.
Placing the development users into one or more LDAP groups, allows the administrator to grant the groups the required authorizations to the environment in a manifest. If a development group later does not appear in the production manifest, the users' authorizations on the environment are assumed by the production administrators and users that are specified in the manifest.
End users generally do not require authorization to access the solution while it is being built within a development environment. However, their authorizations should become active during the testing phases in an IT or UAT/Preproduction environment so that security testing can be accomplished prior to full production deployment.

Planning

Each target environment is configured individually with a target object store. If a target object store needs more security, authorization must be assigned by specific groups of users instead of allowing all authenticated users. That is, security cannot be assigned by using the #AUTHENTICATED-USERS group. IBM Case Manager recommends that one or more master groups be specified during creation of the target object store and that basic access rights are granted as shown in the following picture. This usage of master groups effectively controls the authorizations for the entire object store on who can use the target object store by adjust the LDAP groups and users membership within the master groups and reducing security configuration complexity. Otherwise, it is harder to add unplanned object store groups and users once the object store has been created and has been in use for a while.
The IBM Case Manager configuration tool and administration client generates a warning if there is no group or user with basic access rights to the target object store.



Administrative Authorizations

The administrators responsible for implementing the security must have the proper authorizations to implement the solution and apply its security. IT administrators and solution administrators must have full control on the target object store of the Case Foundation Server to:

- Deploy solutions

- Configure and update security configurations

The Case Foundation Server has additional built-in configuration groups that are used to provide access to the workflow system. These groups are independent of the IBM Case Manager security configuration. So, these administrative groups and users must be added to the Process Services Administration and Configuration groups within Case Foundation.
As with end user and developer authorizations, different administrators might manage the different target environments. When this situation occurs, the security manifests must be configured to allow the right people the right authorizations accordingly.

Nonadministrative Authorizations

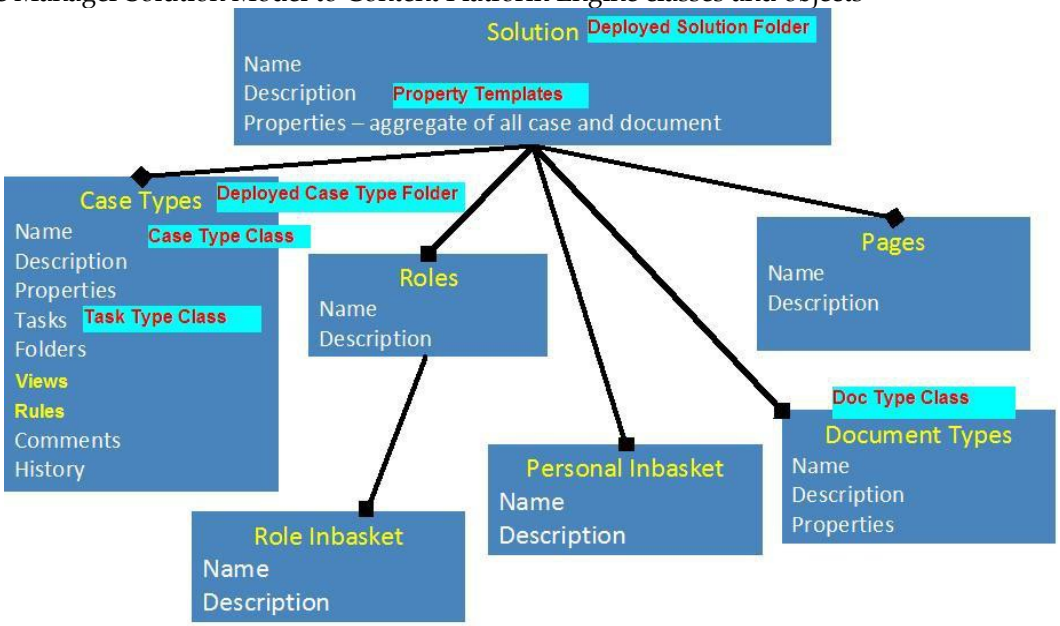
The remaining sections in this article focus on the case management security model and configuration with nonadministrative rights within the target environment. This configuration determines how a user can see and act in terms of case management operations from within Case Manager Client.

IBM Case Manager Solution Deployment to Case Foundation Server

Other objects that are influenced by the Case Manager Client user interface are shown in the following diagram.
In this diagram, we can see the following artifacts deployed to the Content Platform Engine:

Solution - Deployed Solution Folder and Property Templates
Case Types - Deployed Case Type Folder, Case Type Class, and Task Type Class.
Document Types - Doc Type class

IBM Case Manager Solution Model to Content Platform Engine classes and objects

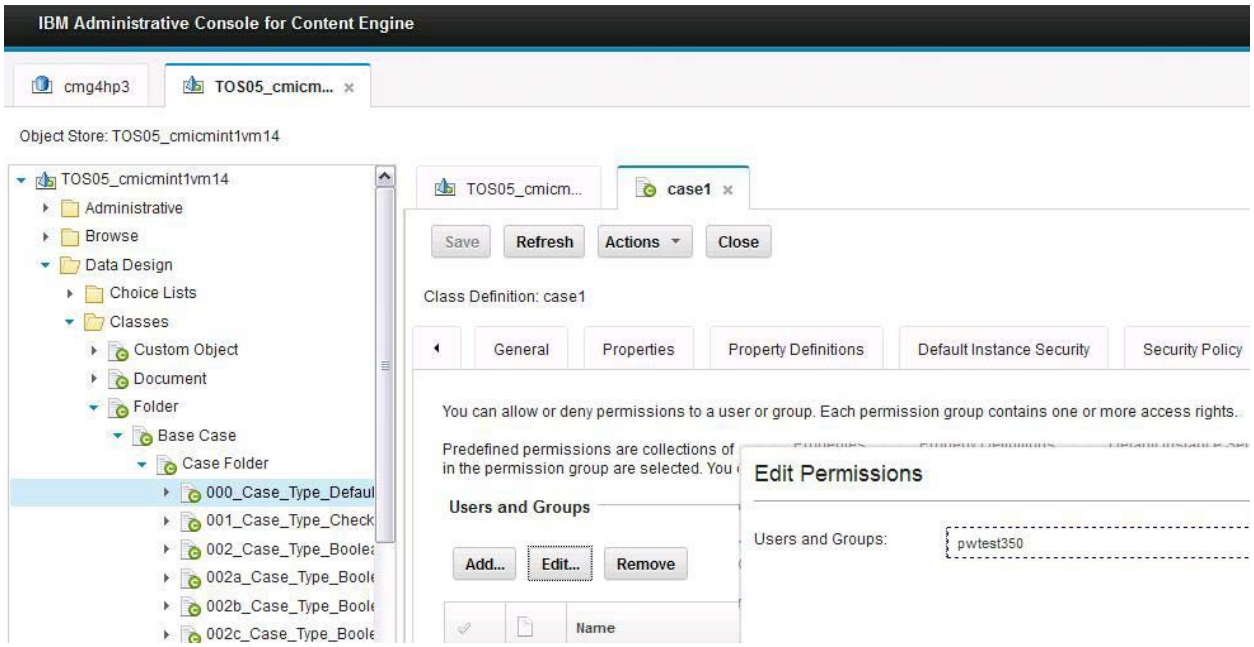


Case Foundation Server Create Instance Rights

The class definition controls:

- Who can view the class
- Who can create an instance of the class

Figure 14-2 Case Type Class Security



The following are IBM Case Manager object classes

IBM Case Manager Object Classes	Description
Case Type	Solution Case Types are subclasses of Case Folder. In addition, the Deployed Case Type folder security to be configured.
Case Subfolder	No subclasses, all object store users can create a case subfolder. In addition, the subfolder right on case or case subfolder must be created.
Document Type	Solution Document Types are subclasses of Document. In addition, the File in Folder right must be defined on the case or case subfolder to allow users to add documents to a case.
Task Types	Solution Task Types are subclasses of Case Task. In addition, the Process Services Roster create right must be set.
Dynamic Task	There is one subclass for each Case Type

	enabled for Dynamic Task. In addition, the Process Services Roster create right must be set.
Comments	All object store users can create comments. In addition, the Annotate right on the case must be set to allow users to add case comments.

Default Instance versus Dynamic Security

When a content object class is created, it is assigned a security model that is automatically applied to new instances of the object. This *default instance security* is modified by the user when he or she creates an instance of that object class. For IBM Case Manager, applying security to every case object can be accomplished the same way directly. However, IBM Case Manager recommends that you use dynamic security instead.

Dynamic security occurs when an object inherits its security from its parent security structure within the object store. When security is changed on the parent security proxy object, the security is recomputed and applied to the child objects.

- If invoiceA is stored in scans, Thomas can view it.
- If invoiceA is moved from scans to invoices, Thomas cannot view it.
- If invoiceA is filed on both scans and invoices so that it resides in both folders, Thomas can view it.

Dynamic, or inherited security, reduces the amount of authorization configuration that is required for case management because all objects that are related to a given case are generally stored in the case folder structure. This allows the IBM Case Manager administrator to define security manifests for the case folder structure without forcing the administrator to deal with the security of individual case subfolder, tasks, and comments within the case.

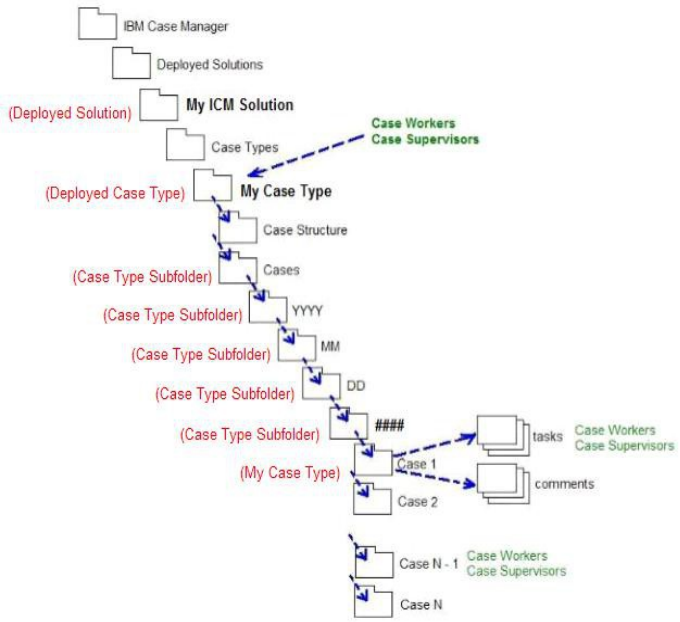
While dynamic security is preferred, its use does not preclude the direct application of authorizations to any object. Where required, users have the ability to apply special authorizations that deny access to a given content item. Once access is denied, an item can be accessed by the denied user only by changing the authorization that denies access. Hence, denying access to an object through LDAP groups must be carefully applied.

Direct access control requires careful planning because the underlying security model is directly applied. If you have a large number of cases and case child objects for which security needs to be changed, the direct access control security model becomes very difficult and tedious to update.

Using the dynamic security model allows the security to be configured for the deployed case type folder. Security is then inherited cleanly all the way down. Future updates or changes to security across all existing instances is streamlined when dynamic security is used. Each case can contain many related case objects whose security modification is easily reflected by changing the security only for the deployed case type folder to propagate down the substructure and the objects within the entire structure.

Dynamic security inheritance allows changes of security that can be triggered by any personnel functional responsibility change, corporate structural reorganization, business model or requirement update, or government mandates, and so on. Because only a fixed number of well-known control points need their security updated for the platform to reflect the access control dynamically, efficiently, and reliably.

In IBM Case Manager, the default security model assumes all case instances have same rights as the deployed case type folder. This feature provides consistent security control as shown in the following figure:



Document Security Model

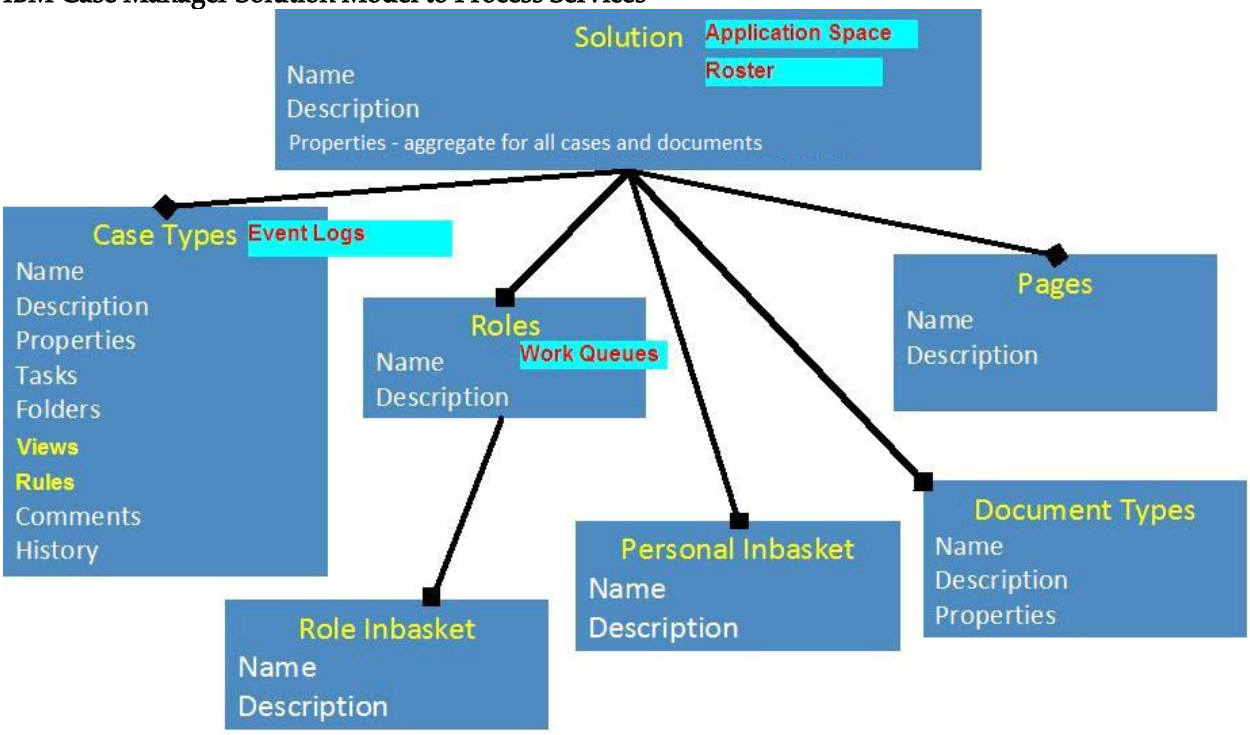
Documents are a critical aspect of any case. Whether the documents are invoices, claims, contracts, or any other case-related document, they all share a common requirement. They must have the proper authorizations applied to allow users to accomplish case activities.

Existing document classes can be reused in a case management solution. When created, each document class already has a default security configuration. Generally, that configuration is unmodified because a single document can be shared and filed in multiple cases. When a document is filed in different cases, its security in general should not be changed as a side-effect to avoid unexpected security concern or issues. For example, if the document user can only view and not modify the document properties or version its content, filing that document into a case should not unnecessarily elevate the user's authorizations.

In IBM Case Manager, case documents still use the standard default instance security model that is controlled by document subclasses.

IBM Case Manager Solution Model to Process Services

The following diagram shows the following elements deployed to Content Platform Engine:
Solution – Application Space, Roster
Case Types – Event Logs
Roles – Work Queues
It is important to note that multiple users may come into the same region. There can be security holes or problems, so it is important to adjust application security. It is important to adjust the application space and role security accordingly. Make sure to set up role membership accordingly.
IBM Case Manager Solution Model to Process Services

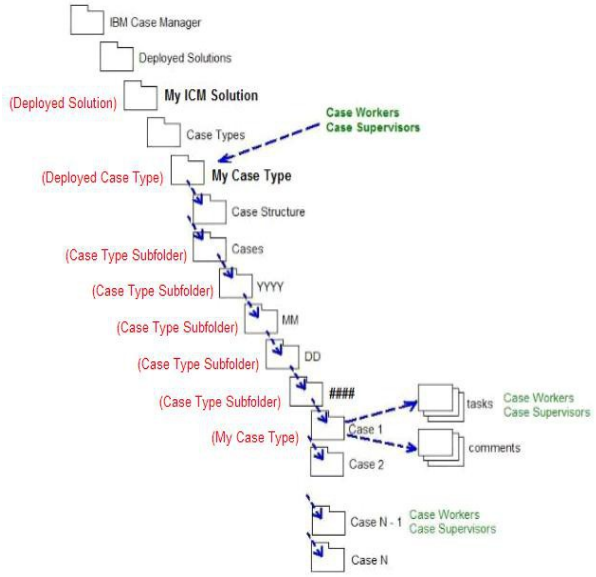


Process Services Security Model

It is important to not leave process services security open. If it is only secured on IBM FileNet Content Manager side, that is not sufficient.
Make sure to setup Process Services Administrator and Configuration groups to IT/IBM Case Manager Solution Administrators.
For the solution application space, users who can manage roles must be added to application space security. Also, there is no longer a need to make adjustments for reassign work to see all roles.
The solution roster controls task process creation and launching. Users who might perform actions such as starting a task during case creation or creating and starting a discretionary or custom task need create privileges.
The event log for each case type is used by the case history and the Timeline Visualizer widget.

The work queue for each role requires query and process rights to get to work objects and to process and dispatch these work objects. On the Content Platform Engine side, security is further influenced by the task processes design and needs to be reviewed. For example, there can be a user who can view and query the work items, select a response, and influence how the work is routed next. However, that user can only view cases and cannot perform actions such as updating case properties and adding documents. There can be another user who can actually update the work item with new values through case properties that are exposed in the step UI as read/write), add documents, create comments, and other perform other actions that need case update rights.

The following diagram shows how the correct security permissions for each role and work queue from the Content Platform Engine now affect the solution and case types:



Component Queue Workers

The IBM Case Manager configuration tool configures the default security for IBM Case Manager component queues including case operations and rule operations. Do not use the Content Platform Engine administrator account for this security. Instead, use a delegated non-full control account for these uses. It is recommended that the Content Platform Engine security for this account be configured to perform the operations such as creating a case, updating case properties, and filing a document.
In addition, customer IT/IBM Case Manager solution administrators must configure security for any additional custom component queues as needed.

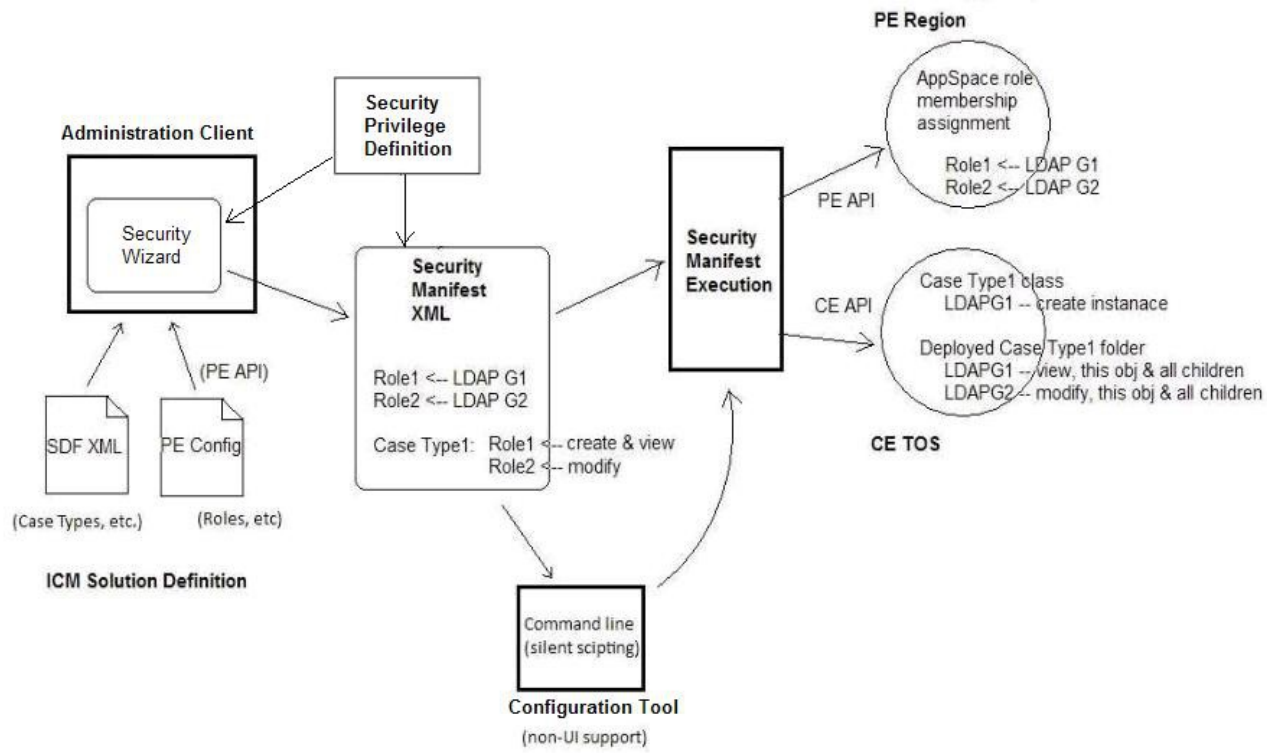
Security Wizard and Customization

Security Wizard Infrastructure and Customization Overview

The IBM Case Manager V5.2 security wizard provides easier configuration of IBM Case Manager solution security without requiring the use of tools such as Administration Console for Content Engine (ACCE) and Process Configuration Console (PCC).
The security wizard is based on IBM Case Manager model layer abstraction. The wizard explores the solution definition and presents the user interface accordingly, based on the solution in context. There is no need to navigate around the tools in ACCE and PCC to find the classes and objects that are related to the solution to be configured.
The security wizard also allows you to apply the IBM Case Manager solution configuration correctly and consistently. The configuration can easily be readjusted and applied repeatedly based on business needs. The solution itself might not have changed or have been redeployed, but security can be changed periodically based on organizational changes, business practices, or mandates. The security wizard also provides good traceability and logs that document what is done to the system.
The security wizard can be customized as IBM Case Manager provides a default privilege definition. This default privilege definition can be customized and cause the security wizard to be reconfigured and reflected in the user interface panels so that the user can customize and fit the wizard to their specific business needs.
The security wizard can be migrated and easily adjusted and applied across multiple systems as opposed to trying to reproduce the security configuration procedure manually, which is error prone. The security wizard can also be scripted to facilitate automated solution deployment and configuration by using the IBM Case Manager configuration tool command line mode.

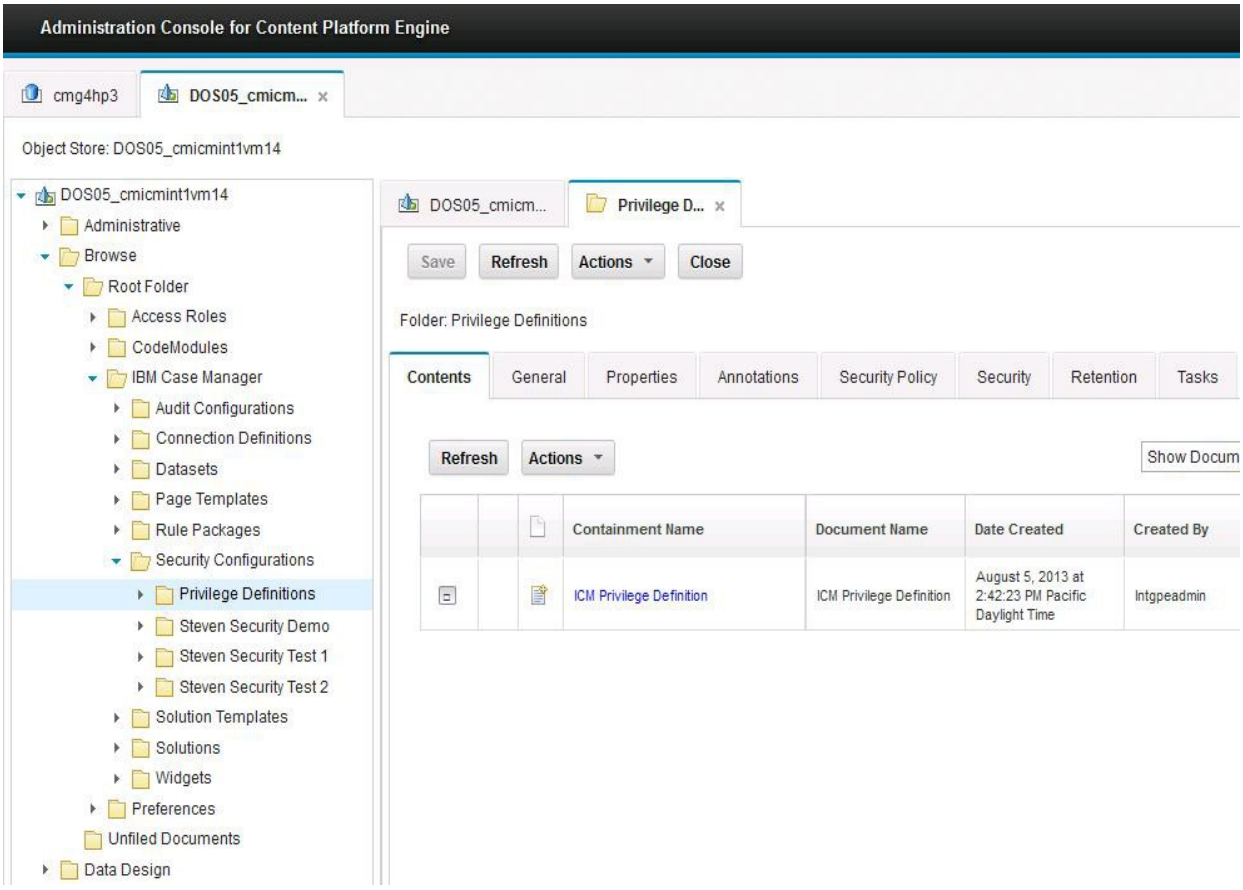
Security Wizard Infrastructure

The following diagram shows how the IBM Case Manager administration client connects to the security wizard. The security wizard reads the solution definition file and presents it within the wizard. This diagram shows how the security privilege definition, the security manifest XML, and the security manifest execution connect together in the security wizard.



Security Privilege Definition

The security privilege definition is in the design object store. The following screen capture shows where you can find the security privilege definition file in the Administration Console for Content Platform Engine.


Administration Console for Content Platform Engine
cmg4hp3
DOS05_cmicm...
Object Store: DOS05_cmicmint1vm14
DOS05_cmicmint1vm14
Administrative
Browse
Root Folder
Access Roles
CodeModules
IBM Case Manager
Audit Configurations
Connection Definitions
Datasets
Page Templates
Rule Packages
Security Configurations
Privilege Definitions
Steven Security Demo
Steven Security Test 1
Steven Security Test 2
Solution Templates
Solutions
Widgets
Preferences
Unfiled Documents
Data Design
DOS05_cmicm...
Privilege D...
Save
Refresh
Actions
Close
Folder: Privilege Definitions
Contents
General
Properties
Annotations
Security Policy
Security
Retention
Tasks
Refresh
Actions
Show Docum
Containment Name
Document Name
Date Created
Created By
ICM Privilege Definition
ICM Privilege Definition
August 5, 2013 at 2:42:23 PM Pacific Daylight Time
Intgpeadmin

IBM Case Manager Privilege Definition

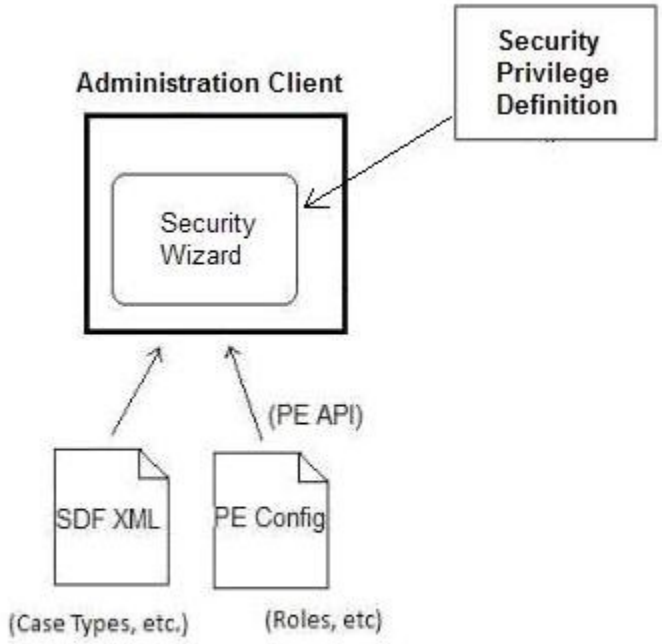
The following screen capture shows the content of the security privilege definition file. Thecomments in the file explain how to customize the file.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Instructions:
- Modify a privilege by adding or removing permissions in <secdef:allow> elements under each <secdef:privilegeDefir

- Remove a privilege from the security configuration wizard by removing the corresponding <secdef:privilegeDefiniti
<secdef:allow> permission child elements.

- Add a new, customized privilege by adding a new <secdef:privilegeDefinition> element with appropriate permission
  In the <secdef:privilegeDefinition> element, specify category="icm" to add the privilege to the "Modify permissic
  security configuration wizard.
  Specify category="admin" to add the privilege to the "Define the administrators and assign privileges" window.

See the topic "Customizing privileges and permissions" in the IBM Case Manager Information Center for information.
-->

<!-- all permissions

<secdef:privilegeDefinitions xmlns:secdef="http://www.ibm.com/xmlns/prod/ecm/acm/secdef">
    <secdef:privilegeDefinition name="create" category="icm">
        <secdef:allow>createCase</secdef:allow>
        <secdef:allow>startTask</secdef:allow>
    </secdef:privilegeDefinition>
    <secdef:privilegeDefinition name="view" category="icm">
        <secdef:allow>viewCase</secdef:allow>
    </secdef:privilegeDefinition>
    <secdef:privilegeDefinition name="update" category="icm">
        <secdef:allow>viewCase</secdef:allow>
        <secdef:allow>updateCase</secdef:allow>
        <secdef:allow>addDocument</secdef:allow>
        <secdef:allow>createSubfolder</secdef:allow>
        <secdef:allow>addComment</secdef:allow>
        <secdef:allow>createDiscretionaryTask</secdef:allow>
        <secdef:allow>createDynamicTask</secdef:allow>
        <secdef:allow>startTask</secdef:allow>
        <secdef:allow>viewWork</secdef:allow>
        <secdef:allow>processWork</secdef:allow>
    </secdef:privilegeDefinition>
    <secdef:privilegeDefinition name="manage" category="icm">
        <secdef:allow>manageCase</secdef:allow>
        <secdef:allow>startTask</secdef:allow>
        <secdef:allow>manageRole</secdef:allow>
    </secdef:privilegeDefinition>
    <secdef:privilegeDefinition name="fullcontrol" category="admin">
        <secdef:allow>fullControl</secdef:allow>
    </secdef:privilegeDefinition>
</secdef:privilegeDefinitions>
```

Security Wizard Infrastructure

The security wizard user interface is based on the solution definition and the security privilege definition. You can modify the permissions for roles and specify what kind of rights each role has to create cases, view cases, update cases, and manage cases.

For example, in the following screen capture, the partner can only view a case.




```
- <secdef:privilegeDefinitions xmlns:secdef="http://www.ibm.com/xmlns/prod/ecm/a
  - <secdef:privilegeDefinition category="icm" name="create">
      <secdef:allow>createCase</secdef:allow>
      <secdef:allow>startTask</secdef:allow>
    </secdef:privilegeDefinition>
  + <secdef:privilegeDefinition category="icm" name="view">
  + <secdef:privilegeDefinition category="icm" name="update">
  + <secdef:privilegeDefinition category="icm" name="manage">
  + <secdef:privilegeDefinition category="admin" name="fullcontrol">
</secdef:privilegeDefinitions>
```

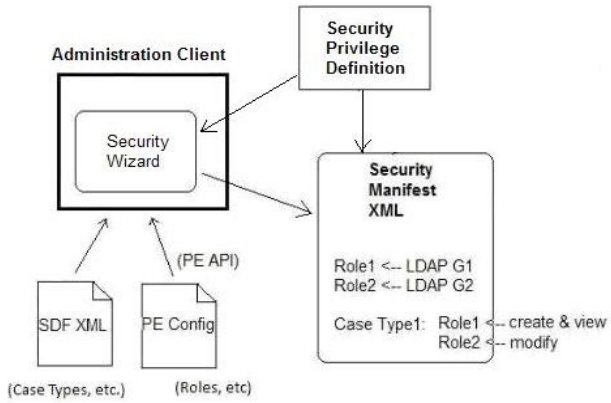
Modify permissions for roles

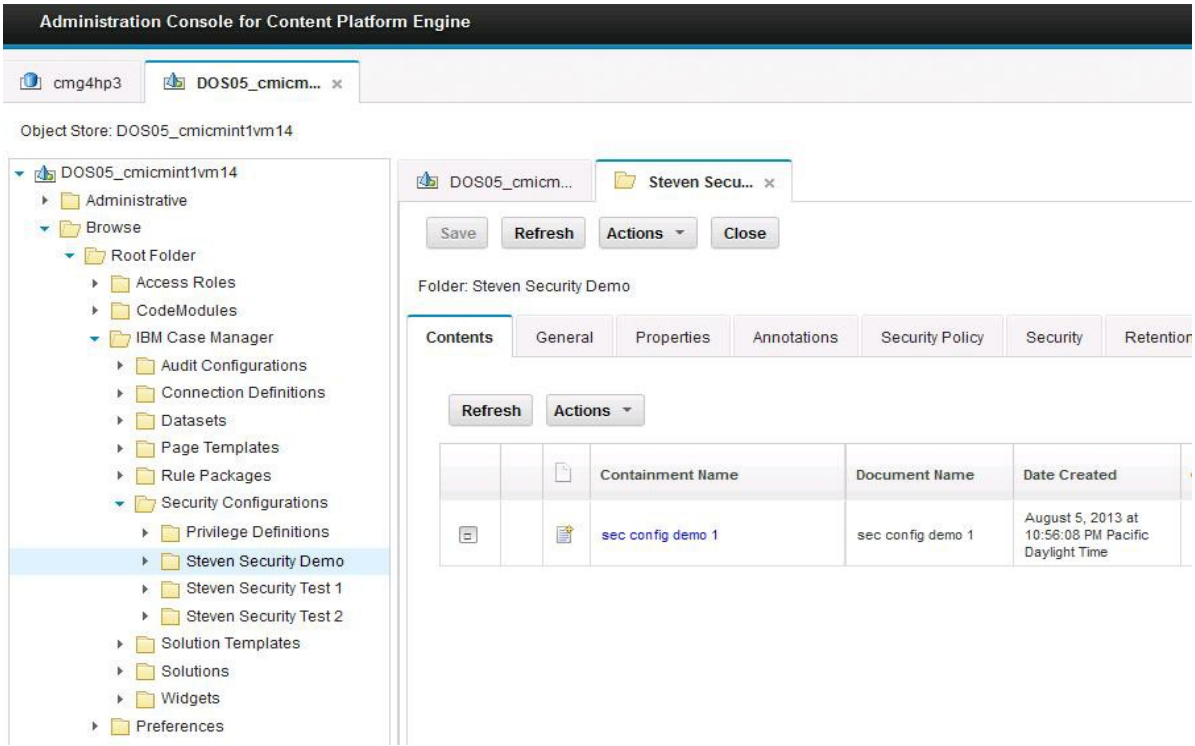
Expand All | Collapse All | Add | Remove

Case Type	Role	Create Case	View Case	Update Case	Manage Case
▸ All Case Types					
▾ case2					
	Partner	☐	☑	☐	☐
	Worker	☑	☐	☑	☐
Discovered from Solution Definition	Supervisor	☑	☐	☑	☐
	Manager	☐	☐	☐	☑
	Auditor	☐	☑	☐	☐

Security Configuration/Manifest

For each solution under the Security Configurations folder, the security configuration/manifest file is saved as shown in the following screen capture. The security configuration/manifest is specific for each solution and that is why the manifests are sorted by solutions.
In most common use case, there is one security configuration/manifest that is under versioning. If the same solution is deployed to different regional centers across geographies, you can have different security configuration/manifests.



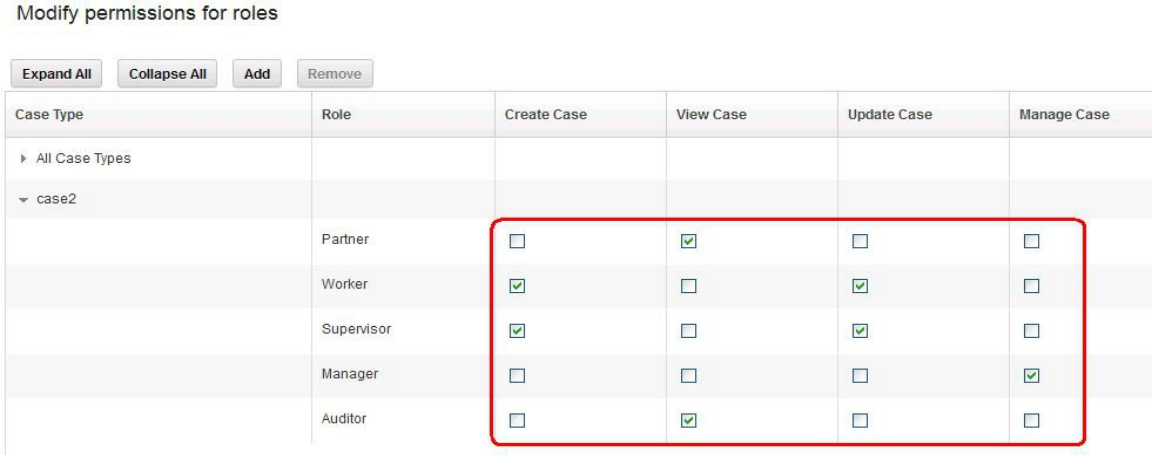


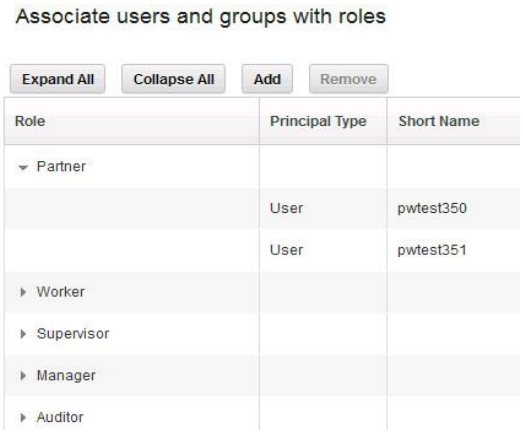
The following screen capture shows the contents of the security manifest XML file.

In the security manifest XML file, each role is defined along with the privileges that are assigned to each role.

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <sec:securityManifest xmlns:cmis="http://docs.oasis-open.org/ns/cmis/core/200908/" xmlns:sec="http://www.ibm.co
xmlns:caseext="http://www.ibm.com/xmlns/prod/ecm/cmis/caseextensions">
    <sec:privilegeDefinition>{5EF45597-863E-4D82-A97F-448F36CEFDF5}</sec:privilegeDefinition>
  - <sec:roleMembership role="Partner">
      <sec:ldapUser>pwtest350</sec:ldapUser>
      <sec:ldapUser>pwtest351</sec:ldapUser>
    </sec:roleMembership>
  + <sec:roleMembership role="Worker">
  + <sec:roleMembership role="Supervisor">
  + <sec:roleMembership role="Manager">
  + <sec:roleMembership role="Auditor">
  + <sec:solution>
  + <sec:solution>
  + <sec:solution>
  + <sec:solution>
  + <sec:solution>
  - <sec:caseType name="SSD_case2">
      - <sec:role name="Partner">
          <sec:privilege name="view"/>
        </sec:role>
      - <sec:role name="Worker">
          <sec:privilege name="create"/>
          <sec:privilege name="update"/>
        </sec:role>
      - <sec:role name="Supervisor">
          <sec:privilege name="create"/>
          <sec:privilege name="update"/>
        </sec:role>
      - <sec:role name="Manager">
          <sec:privilege name="manage"/>
        </sec:role>
      - <sec:role name="Auditor">
          <sec:privilege name="view"/>
        </sec:role>
    </sec:caseType>
  + <sec:administrator name="Intgpeadmin">
  - <sec:administrator name="pwtestadmin">
      <sec:ldapUser>pwtestadmin</sec:ldapUser>
      <sec:privilege name="fullcontrol"/>
    </sec:administrator>
    <sec:applyRoleMembership>true</sec:applyRoleMembership>
    <sec:applyAllDiscretionaryTasks>true</sec:applyAllDiscretionaryTasks>
</sec:securityManifest>
```

The following screen capture shows the graphical user interface that allows users to set different permissions for each role.

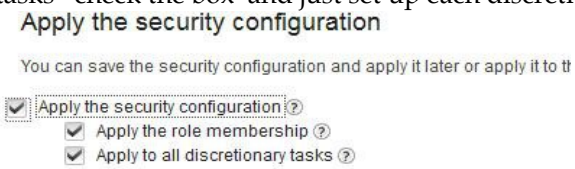




The following screen capture shows how to define the administrators and assign privileges based on users. However, you typically have the Administration Group added here instead.

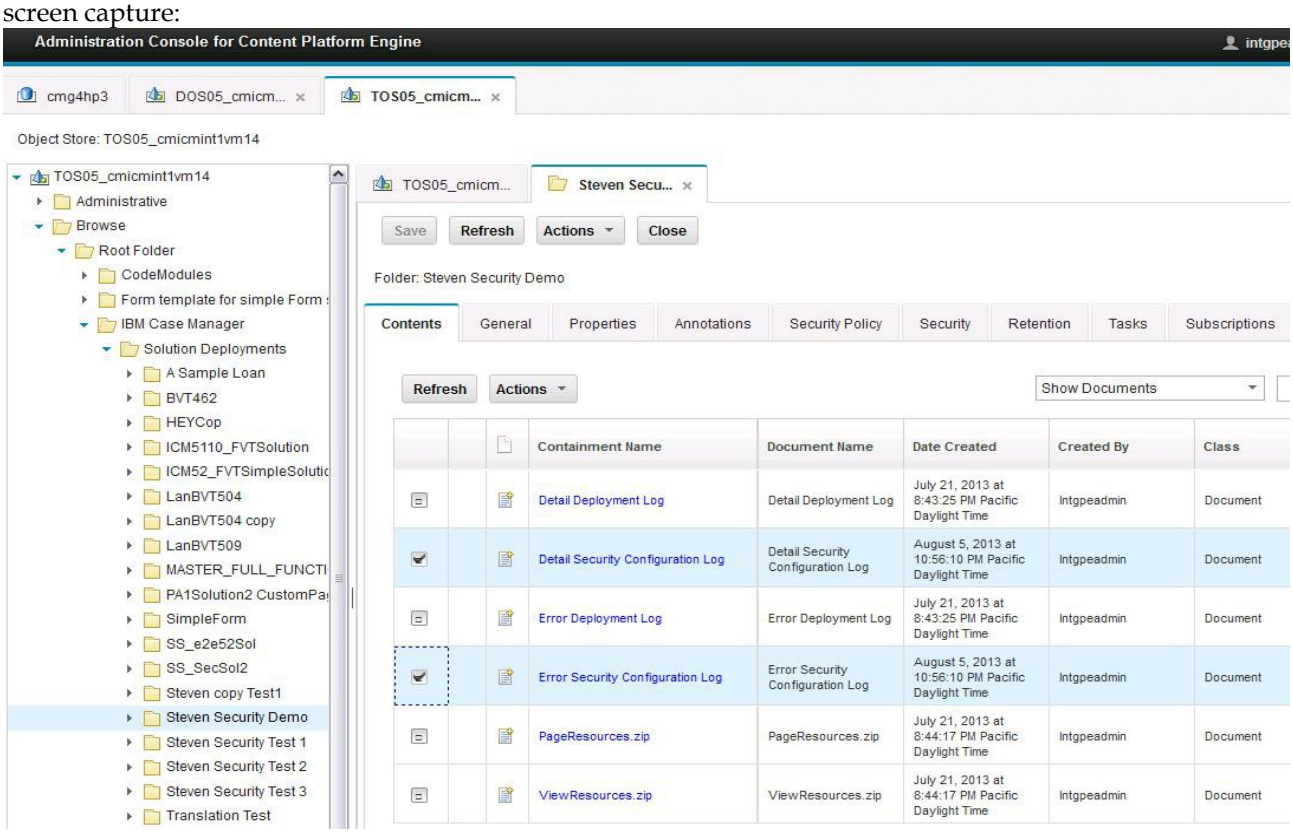
Apply Security Configuration

Clear the "Apply the role membership" check box if you are using Case Manager Client-enabled Manage Roles to prevent overriding the security settings.
The "Apply to all discretionary tasks" checkbox uses the security wizard to configure all discretionary tasks
The following screen capture shows the final part of the security wizard if you want to apply the security configuration to the role membership to all discretionary tasks. The best practice is then to manually adjust the rights to create instances for some discretionary tasks by using ACCE as needed. If you are manually adjusting many create instance exceptions, then do not select the "Apply to all discretionary tasks" check the box and just set up each discretionary task accordingly.



After Security Configuration Execution – Logs

There are additional error and detail security logs that are created and located as shown in the following screen capture:



Customization of Privileges and Permissions

When assigning authorizations for the roles that are associated with a solution, the administrator chooses permissions in the IBM Case Manager administration client security configuration wizard. Each privilege consists of one or more permissions that is within a privilege definition file. The privilege definition file aggregates the underlying Content Platform Engine permissions to assign case authorizations easily.
For example, if you want to add the "view and comment" privilege, you can add the following text to the privilege definition file:

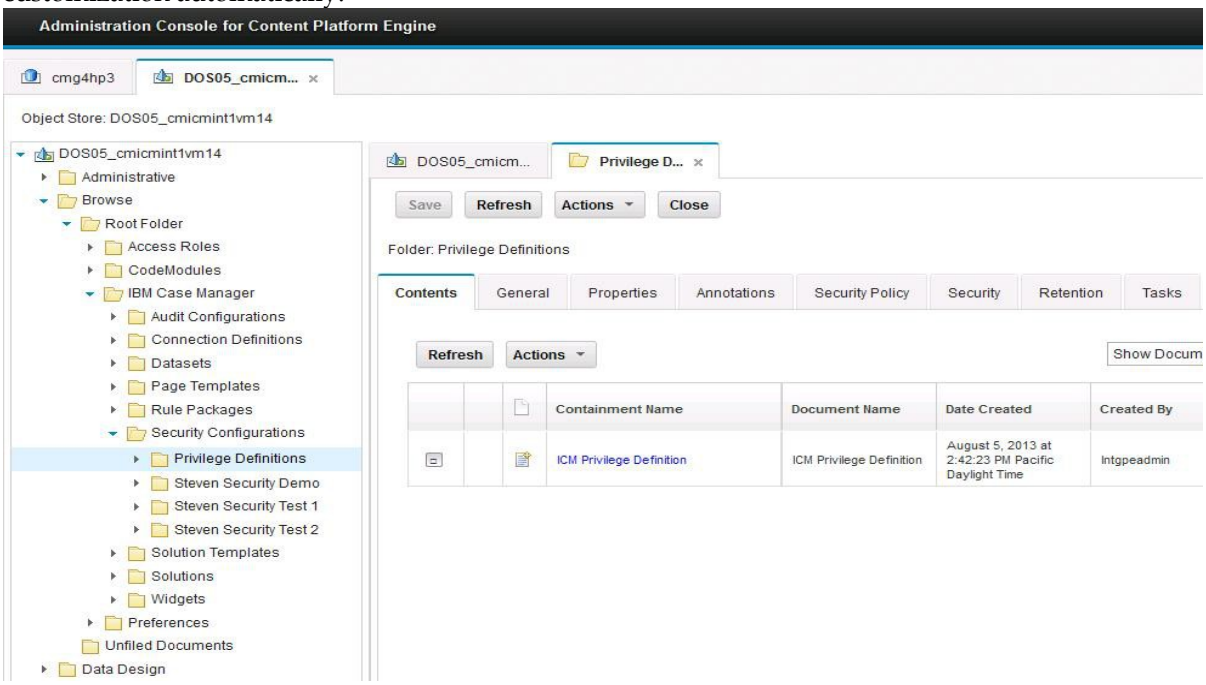
```
<secdef:privilegeDefinition name="view and comment" category="icm">
        <secdef:allow>viewCase</secdef:allow>
        <secdef:allow>addComment</secdef:allow>
</secdef:privilegeDefinition>
```

The privilege definition file provides the ability to add or remove for the create, view, update, manage, and full control case manager authorizations. These authorizations are the basis for the role security within the case manager application.
An organization can choose to modify the privilege definition file to suit their specific needs by adding or removing authorization mappings. When the privilege definition file is modified, the administrators must synchronize the privilege definition file within the various environments.

For more details, see the IBM Case Manager v5.2 Information Center:
http://www-01.ibm.com/support/knowledgecenter/SSCTJ4_5.2.0/com.ibm.casemgmt.design.doc/acmsc003.htm

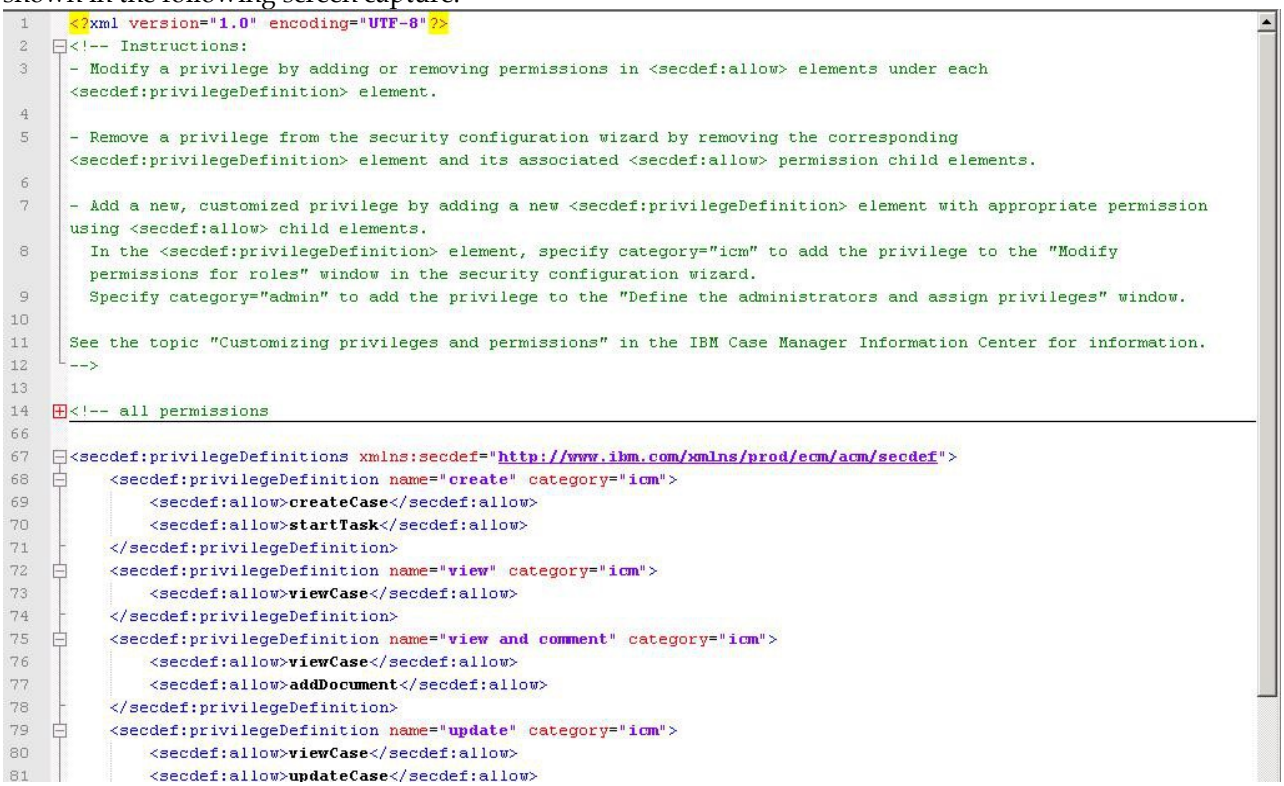
Customization Procedure

To begin customizing the IBM Case Manager privilege definition, first navigate to the IBM Case Manager privilege definition as shown in the following screen capture. Then, check out and download the current definition. Then you can customize and edit the IBM Case Manager privilege definition. Once finished, check in the IBM Case Manager privilege definition and the security wizard user interface reflects the customization automatically.



Customization Instructions

There are some customization instructions that is available in the security configuration definition file as shown in the following screen capture.



```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Instructions:
- Modify a privilege by adding or removing permissions in <secdef:allow> elements under each
<secdef:privilegeDefinition> element.

- Remove a privilege from the security configuration wizard by removing the corresponding
<secdef:privilegeDefinition> element and its associated <secdef:allow> permission child elements.

- Add a new, customized privilege by adding a new <secdef:privilegeDefinition> element with appropriate permission
using <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.

See the topic "Customizing privileges and permissions" in the IBM Case Manager Information Center for information.
-->

<!-- all permissions

<secdef:privilegeDefinitions xmlns:secdef="http://www.ibm.com/xmlns/prod/ecm/acm/secdef">
    <secdef:privilegeDefinition name="create" category="icm">
        <secdef:allow>createCase</secdef:allow>
        <secdef:allow>startTask</secdef:allow>
    </secdef:privilegeDefinition>
    <secdef:privilegeDefinition name="view" category="icm">
        <secdef:allow>viewCase</secdef:allow>
    </secdef:privilegeDefinition>
    <secdef:privilegeDefinition name="view and comment" category="icm">
        <secdef:allow>viewCase</secdef:allow>
        <secdef:allow>addDocument</secdef:allow>
    </secdef:privilegeDefinition>
    <secdef:privilegeDefinition name="update" category="icm">
        <secdef:allow>viewCase</secdef:allow>
        <secdef:allow>updateCase</secdef:allow>
```

Understand the Permissions

There are more granular security configuration and privileges that can be fine-tuned in the security configuration file as shown in the following screen capture.

For example, lines 20-21 show how to set the “view all properties” and “read permissions” rights on a deployed case type folder and applies to “this object and all children.”

```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <!-- Instructions:
13
14 <!-- all permissions
15     <allow>createCase</allow>
16     - Sets the "view all properties," "create instance," and "read permissions" rights on a case type subclass and
       applies to "this object only"
17     - Sets the "modify all properties" right on a deployed case type folder and applies to "this object only"
       (note: in order to update CmAcmSequenceNumber)
18     - Sets the "view all properties," "create subfolder," "file in folder/annotate," and "read permissions" rights
       on a deployed case type folder and applies to "this object and all children"
19
20     <allow>viewCase</allow>
21     - Sets the "view all properties" and "read permissions" rights on a deployed case type folder and applies to
       "this object and all children"
22
23     The following permissions also require the <allow>viewCase</allow> element to be able to initially retrieve to a
       case:
24     <allow>updateCase</allow>
25     - Sets the "modify all properties" right on a deployed case type folder and applies to "this object and all
       children"
26     <allow>createSubfolder</allow>
27     - Sets the "create subfolder" right on a deployed case type folder and applies to "this object and all children"
28     <allow>addComment</allow>
29     - Sets the "file in folder/annotate" right on deployed case type folder and applies to "this object and all
       children"
30     <allow>addDocument</allow>
31     - Sets the "file in folder/annotate" and "unfile from folder" rights on a deployed case type folder and applies
       to "this object and all children"
32     <allow>createDiscretionaryTask</allow>
33     - This permission also requires the <allow>startTask</allow> element
34     - If "Apply to all discretionary tasks" is selected when applying security configuration in the security
       configuration wizard:
35         - Sets the "view all properties," "create instance," and "read permissions" rights for all the discretionary
           task type subclasses for a particular case type and applies to "this object only"
36     <allow>createDynamicTask</allow>
37     - This permission also requires the <allow>startTask</allow> element
38     - Sets the "view all properties," "create instance," and "read permissions" rights on the dynamic task type
       subclass for a particular case type and applies to "this object only"
```

IBM Case Manager Privilege Definition

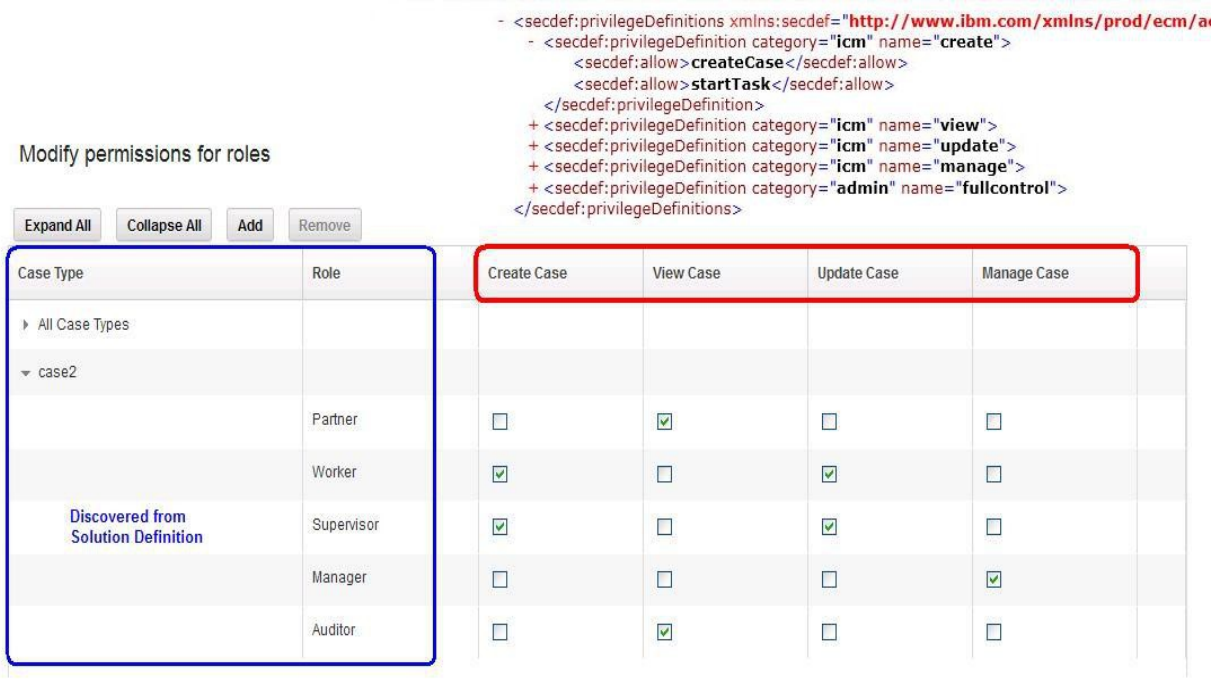
The following screen shot shows the main body of the privilege definition XML. The privilege definitions are defined under “name=create” and so on. We do not recommend changing these values. In the security wizard user interface, there are two categories which are shown as “category=icm” and “category=admin” in the following XML file.

IBM Case Manager and admin are separate panels.

```
<secdef:privilegeDefinitions xmlns:secdef="http://www.ibm.com/xmlns/prod/ecm/acm/secdef">
    <secdef:privilegeDefinition name="create" category="icm">
        <secdef:allow>createCase</secdef:allow>
        <secdef:allow>startTask</secdef:allow>
    </secdef:privilegeDefinition>
    <secdef:privilegeDefinition name="view" category="icm">
        <secdef:allow>viewCase</secdef:allow>
    </secdef:privilegeDefinition>
    <secdef:privilegeDefinition name="update" category="icm">
        <secdef:allow>viewCase</secdef:allow>
        <secdef:allow>updateCase</secdef:allow>
        <secdef:allow>addDocument</secdef:allow>
        <secdef:allow>createSubfolder</secdef:allow>
        <secdef:allow>addComment</secdef:allow>
        <secdef:allow>createDiscretionaryTask</secdef:allow>
        <secdef:allow>createDynamicTask</secdef:allow>
        <secdef:allow>startTask</secdef:allow>
        <secdef:allow>viewWork</secdef:allow>
        <secdef:allow>processWork</secdef:allow>
    </secdef:privilegeDefinition>
    <secdef:privilegeDefinition name="manage" category="icm">
        <secdef:allow>manageCase</secdef:allow>
        <secdef:allow>startTask</secdef:allow>
        <secdef:allow>manageRole</secdef:allow>
    </secdef:privilegeDefinition>
    <secdef:privilegeDefinition name="fullcontrol" category="admin">
        <secdef:allow>fullControl</secdef:allow>
    </secdef:privilegeDefinition>
</secdef:privilegeDefinitions>
```

Security Wizard Customization

The admin category corresponds to the Full Control panel in the following screen capture from the Security Wizard user interface. The Full Control section allows you give to full control to certain users and administrators (groups), but you can also customize this accordingly by using the XML file as shown in the second screen capture that follows.



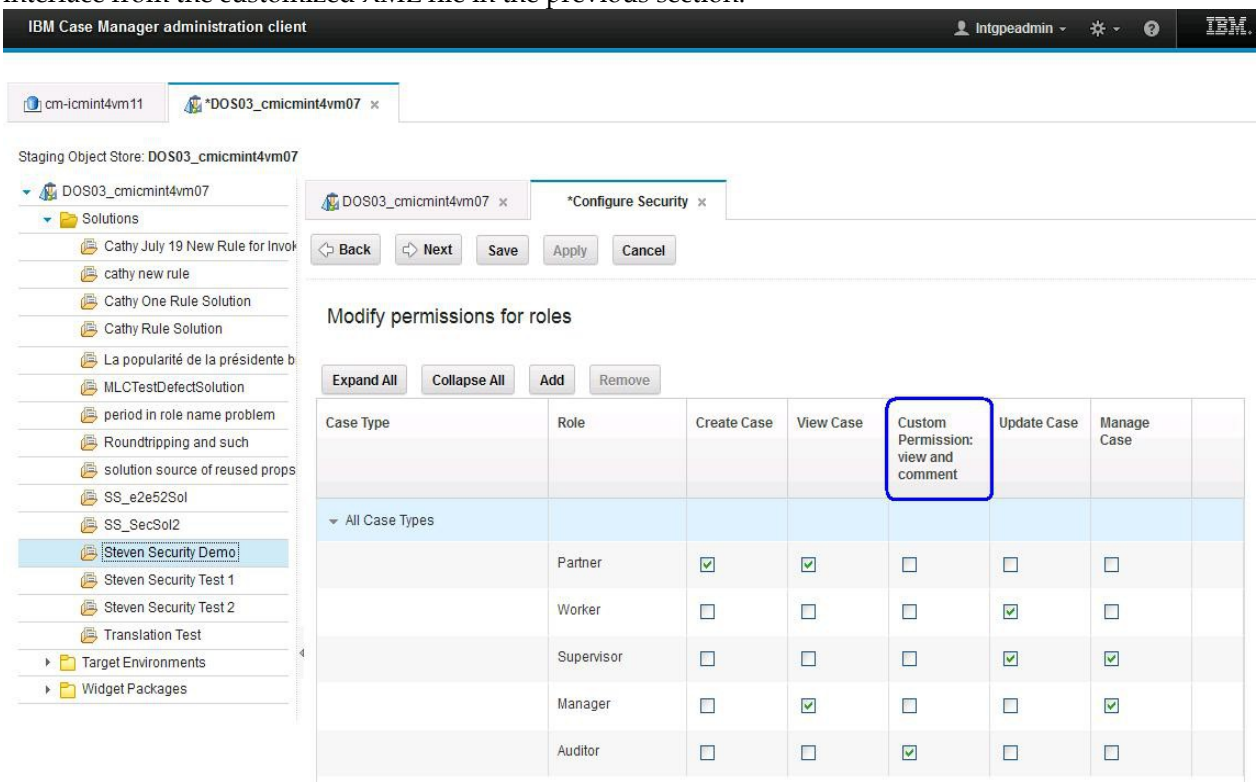
IBM Case Manager Privilege Definition Customization

To customize certain privileges to a certain privilege definition, you can use the XML file. The order presented in this XML file is the order that is presented by the columns for the security wizard user interface.
This ability provides a great quick way to add a privilege to a privilege definition for a certain use case.

```
<secdef:privilegeDefinitions xmlns:secdef="http://www.ibm.com/xmlns/prod/ecm/acm/secdef">
    <secdef:privilegeDefinition name="create" category="icm">
        <secdef:allow>createCase</secdef:allow>
        <secdef:allow>startTask</secdef:allow>
    </secdef:privilegeDefinition>
    <secdef:privilegeDefinition name="view" category="icm">
        <secdef:allow>viewCase</secdef:allow>
    </secdef:privilegeDefinition>
    <secdef:privilegeDefinition name="view and comment" category="icm">
        <secdef:allow>viewCase</secdef:allow>
        <secdef:allow>addComment</secdef:allow>
    </secdef:privilegeDefinition>
    <secdef:privilegeDefinition name="update" category="icm">
        <secdef:allow>viewCase</secdef:allow>
        <secdef:allow>updateCase</secdef:allow>
        <secdef:allow>addDocument</secdef:allow>
        <secdef:allow>createSubfolder</secdef:allow>
        <secdef:allow>addComment</secdef:allow>
        <secdef:allow>createDiscretionaryTask</secdef:allow>
        <secdef:allow>createDynamicTask</secdef:allow>
        <secdef:allow>startTask</secdef:allow>
        <secdef:allow>viewWork</secdef:allow>
        <secdef:allow>processWork</secdef:allow>
    </secdef:privilegeDefinition>
    <secdef:privilegeDefinition name="manage" category="icm">
    <secdef:privilegeDefinition name="fullcontrol" category="admin">
</secdef:privilegeDefinitions>
```

Security Wizard UI Reflects the Customization

The following screen capture shows the custom permission that is displayed in the security wizard user interface from the customized XML file in the previous section.



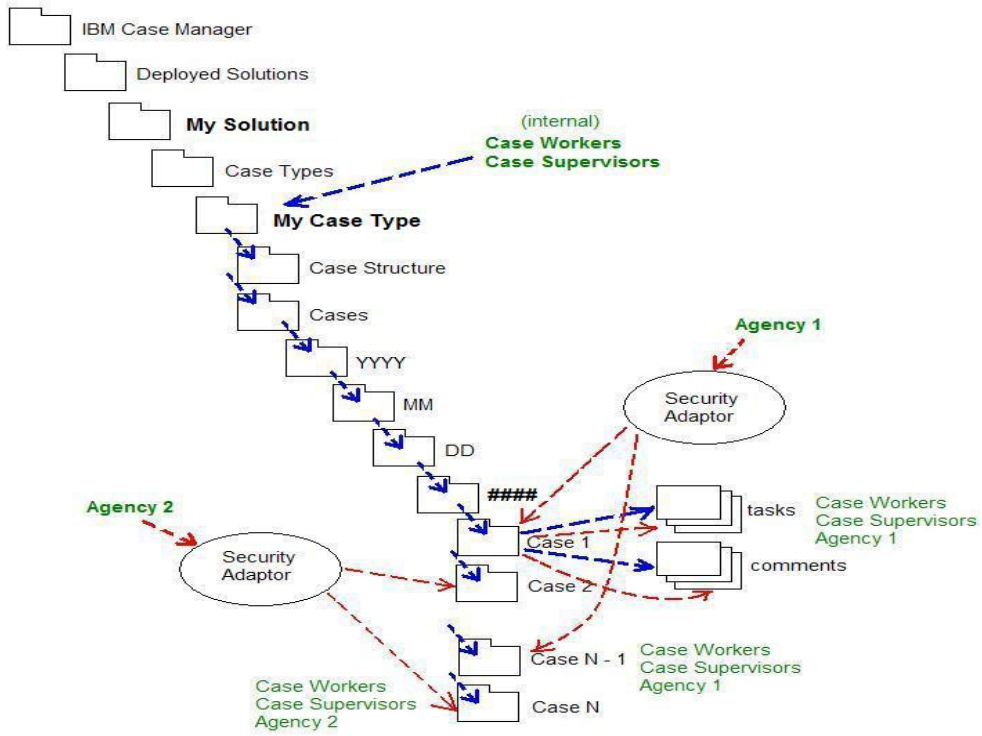
Additional Security Best Practices and Use Cases

The following use cases and best practices have been compiled from various customer engagement and findings so that the user can apply them to IBM Case Manager V5.2.

Security Adaptor/Proxy Hierarchy

The use case in this scenario is that the the user requires case instances of the same case type to have different security. The user would like the same security across case instances, but they might have outside agencies or partners with different requirements.

The following diagram shows how each agency sees only a subset of case instances. For example, agency 2 can see only case 2 and case N.

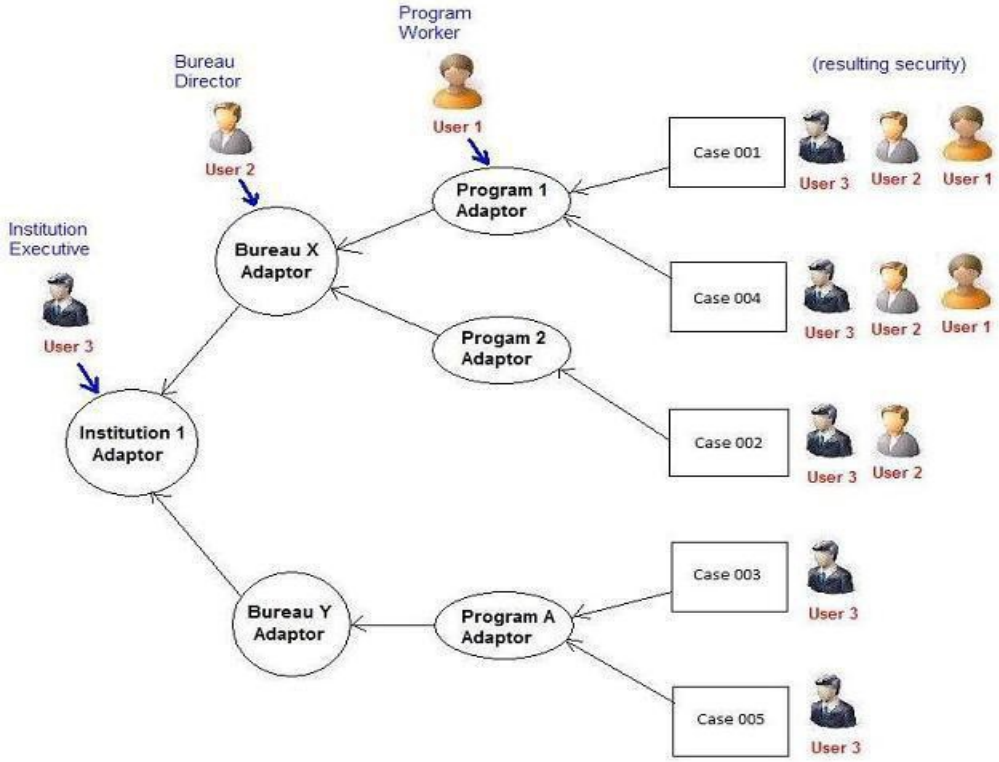


For this use case, IBM Case Manager advises that the customer mix in additional security adaptor/proxy objects. For each case type, they can add an additional object value property that points to the security adaptor/proxy object that allows additonal security to be propagate and applied to case instances selectively.

For preceding example, agency 1 references the security adapter that points to case instances that are different from agency 2 cases and are secured accordingly.

There can be a different structure to an organization as shown in the following diagram. In this use case, different bureaus report up to an institution. IBM Case Manager recommends that the user build a security adaptor hierarchy according to organizational structure or security privilege hierarchy. If shifts in organization require security adjustments, this approach allows a simple adjustment of security proxy pointers (OVPs) to reflect the security changes that are needed.

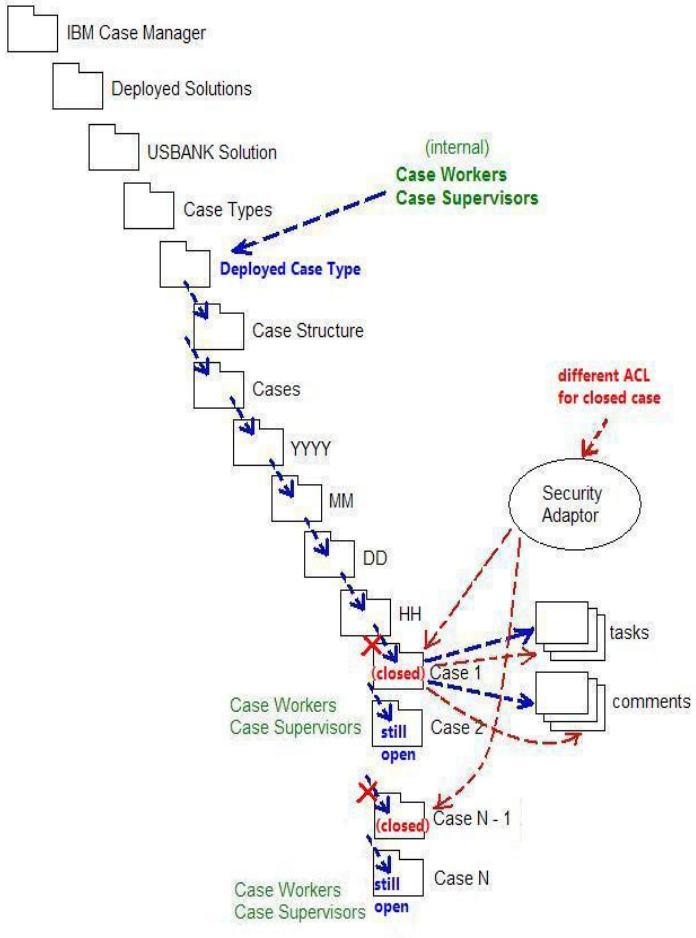
For example, Program 2 can easily be changed to be under the supervision of Bureau Y.



Security Adaptor change based on Case State

In this use case, the user wants to change security when a case reaches a different case state such as a completed or closed state.

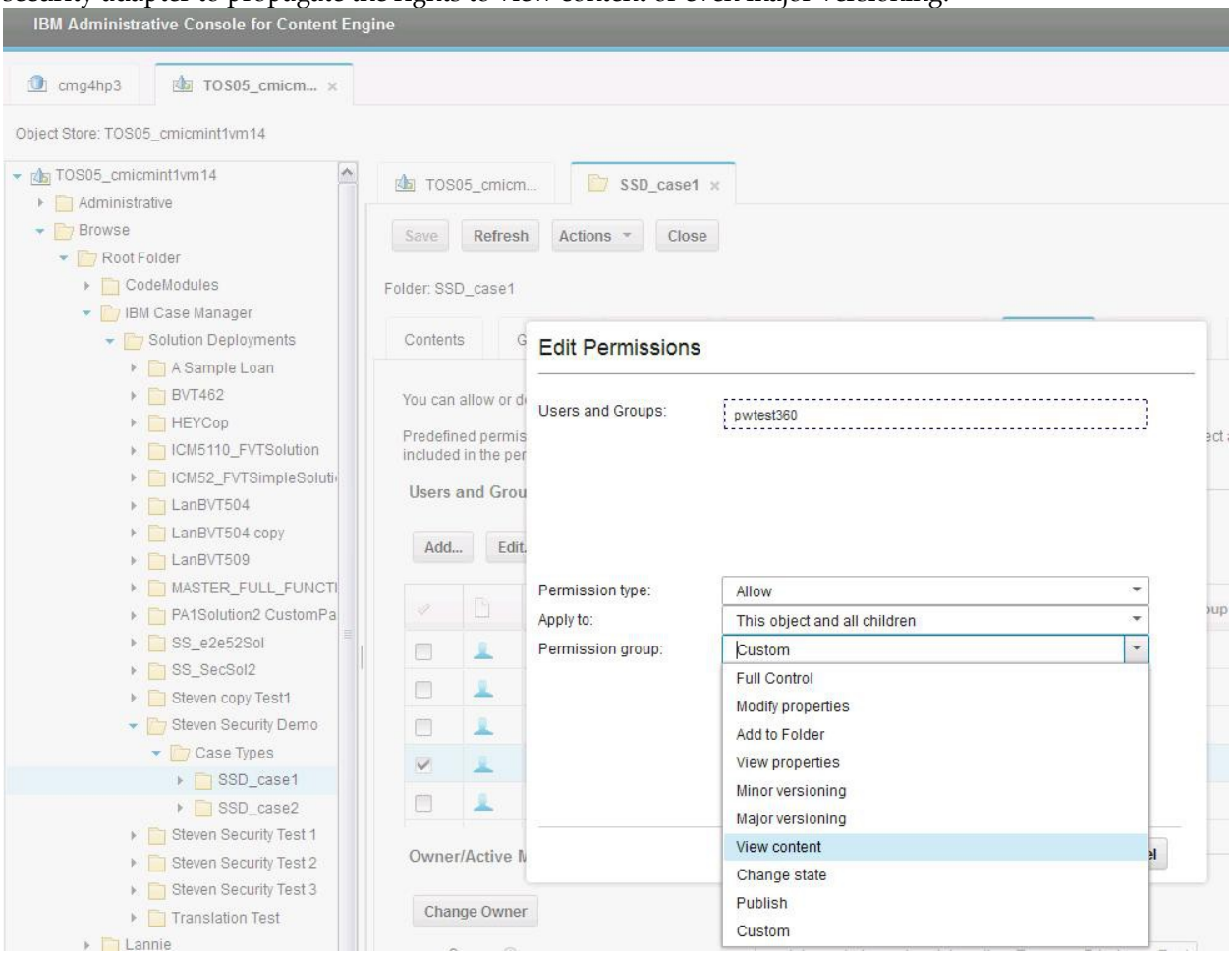
A subset of the cases at different states can have different security rights mixed in or completely replaced.



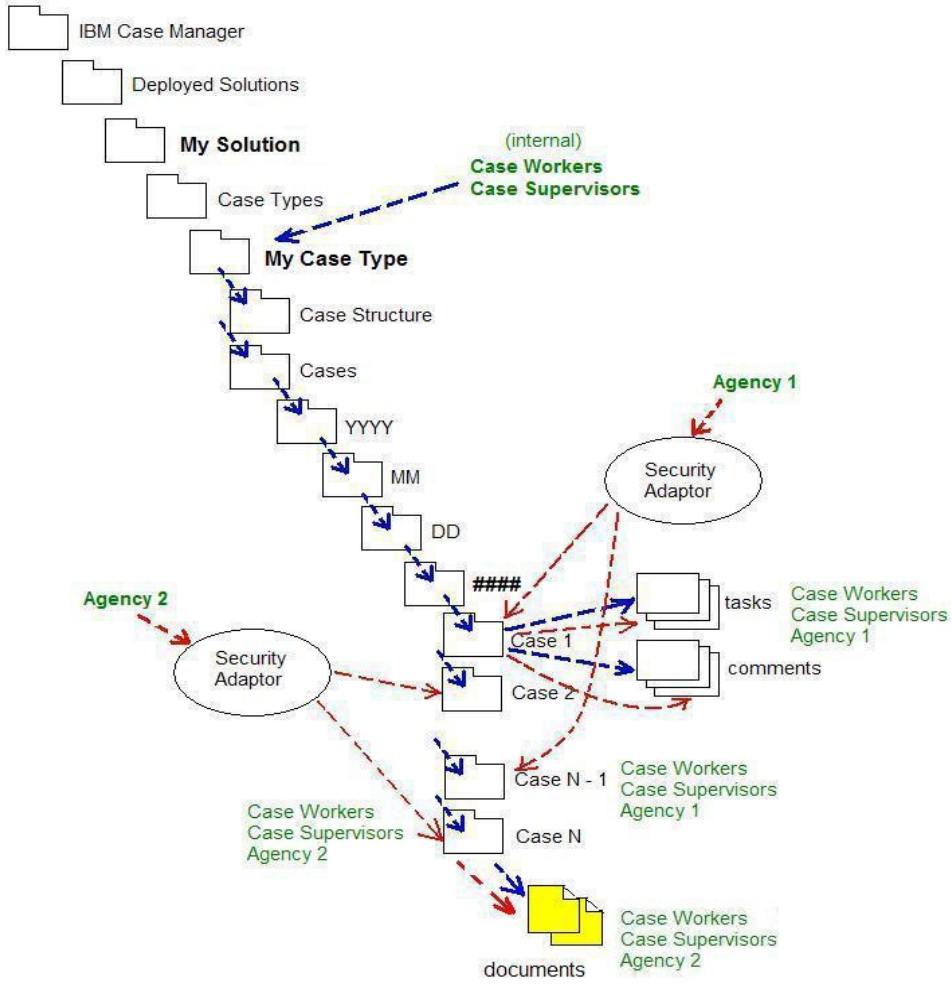
Case Owned Documents

In many case management scenarios, case documents that are added to a case are owned by the case. The documents are there to support that particular case solely, and not shared or filed to any other case.
A common scenario is that when someone is dynamically added to handle a case, that worker can and should be able to view or update any document that is filed in the case.
However, it is not possible to predict all possible document classes involved and the default instance security cannot be predetermined. In addition, it might not be feasible to adjust the security for all document instances whenever a group or user is removed or assigned to handle the case.

In this scenario, IBM Case Manager recommends that you configure the deployed case type folder or security adapter to propagate the rights to view content or even major versioning.



Then, set the security folder of the document to the case folder or case subfolder. This approach allows security to be propagated from container folder to the document as shown in the following diagram:



Export and Import Security Configuration Manifest

For more information about how to export and import the security configuration manifest, see the Solution Deployment Guide developerWorks article at:
https://www.ibm.com/developerworks/community/blogs/e8206aad-10e2-4c49-b00c-fee572815374/entry/ibm_case_manager_5_2_solution_deployment_guide?lang=en

Appendices

References and Acknowledgements

IBM FileNet P8 Version 5.2 Information Center
http://pic.dhe.ibm.com/infocenter/p8docs/v5r2m0/index.jsp
IBM Case Manager Version 5.2 Information Center
http://pic.dhe.ibm.com/infocenter/casemgmt/v5r2m0/index.jsp
IBM FileNet Content Manager Implementation Best Practices and Recommendations
http://www.redbooks.ibm.com/abstracts/sg247547.html
Advanced Case Management with IBM Case Manager
http://www.redbooks.ibm.com/abstracts/sg247929.html

Thank you to the IBMers who contributed ideas and reviewed this guide:

Patricia Sort de Sanz
Bob Jackson
Johnson Liu
Yajie Yang
Wen-Chin (Steven)Hsieh
Yvonne Santiago
Frankie Mosher
Martin Shramo