



1

# IBM Case Manager 5.2 Security Model and Considerations

# Objectives

This session is designed to enable you to:

- ✓Describe the Security Model for Case Management
- ✓Utilize Best Practices for Assigning Security
- ✓Understand how customers are extending security model



# Introduction

- Overview

Focus on the Case Manager security model, best practices and configuration



- Target Audience

Anyone who will be deploying and configuring case solutions in a Production Environment

- Prerequisites

Knowledge of IBM FileNet P8 and Case Manager Architecture

# Session Roadmap

## → Target Environment Security Planning and Configuration

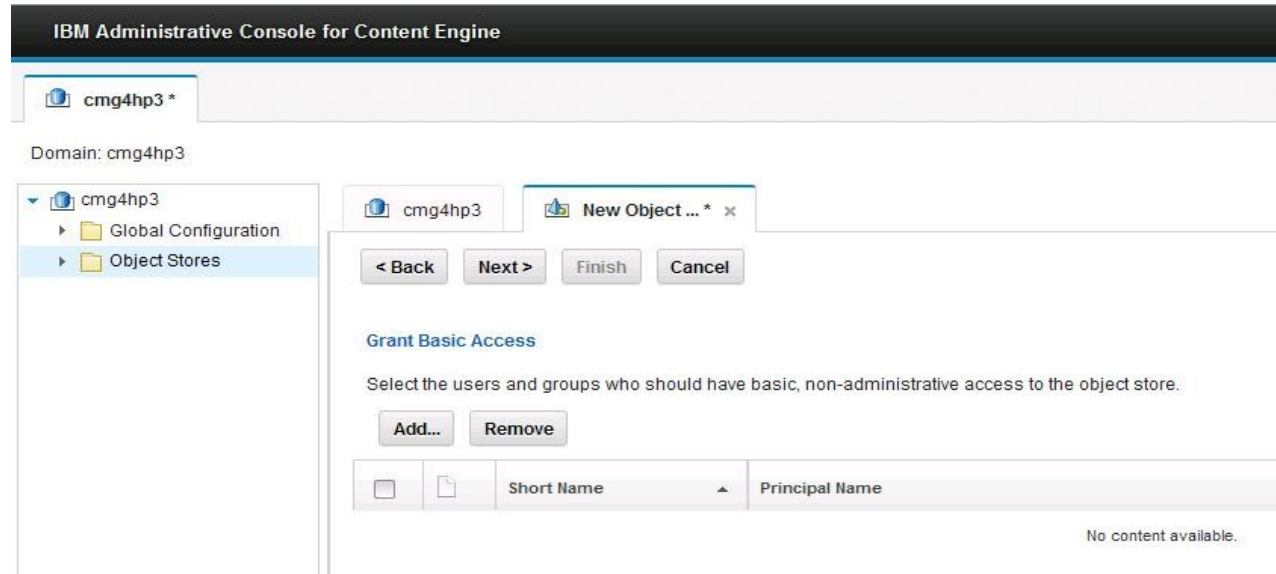
- ICM Solution Model and Solution Structure
- Case Manager Security Model
- Deployed Solutions and Case Client
- Content Engine Classes and Objects
- Process Services Queues, Event Logs, Roster and Application Space
- Additional Security Best Practices
- Q & A

# Target Environment Security Planning

- Security is an important part of system planning
- Plan ahead for groups and/or users who will be accessing the Target Object Store as users
  - If #AUTHENTICATED-USERS cannot be used, then a Master Group (or even Master Groups) should be specified instead during Target Object Store creation time
    - Master group is a LDAP group which in turn contains groups/users
    - Change of access to the OS can then be easily maintained by adding or removing groups/users from the master group within LDAP, which in turn effectively controls the usage of the OS
    - This approach helps setup majority of the basic access rights from OS usage perspective hence minimizes security configuration complexity
  - It will be hard to add unplanned groups/users after the fact to use the OS
    - Customized security scripts or even manual steps are likely involved based on the situation and variations to reach a resolution
    - Consult CPE best practices and recommendation in Info Center
    - Contact IBM subject experts or L2/L3/Enablement team for careful review then plan and apply adjustments accordingly

# Target Environment Creation and Configuration

- Grant #AUTHENTICATED\_USERS or Master Group(s) basic access during OS creation



- Case Manager Configuration Tool and Administration Client checks if there is no group/user with basic access rights at all and generates warning
  - Correct the situation immediately before further proceed with any additional Case Manager configuration steps and OS usage

# Target Environment Administration Security

- Grant IT Administrators and Solution Administrators to have Full Control on CPE to deploy/redeploy solutions, configure/update security configurations and auditing configurations
- Add IT Administrators and Solution Administrators to Process Services Administration and Configuration groups as well

Also

- Security model is an intrinsic part of the solution design
  - What is the problem scenarios to be solved
  - Who the players are for driving the case to resolution
  - How each role involved in the case and perform their work collaboratively
    - What each role can do and what kind of rights needed
- Remaining sections focus on Case Management security model and configuration with non-administrative rights
  - What determines how a user can see and act in terms of Case Management operations from within Case Client

# Session Roadmap

- Target Environment Security Planning and Configuration

- ➔**ICM Solution Model and Solution Structure**

- Case Manager Security Model

- Deployed Solutions and Case Client

- Content Engine Classes and Objects

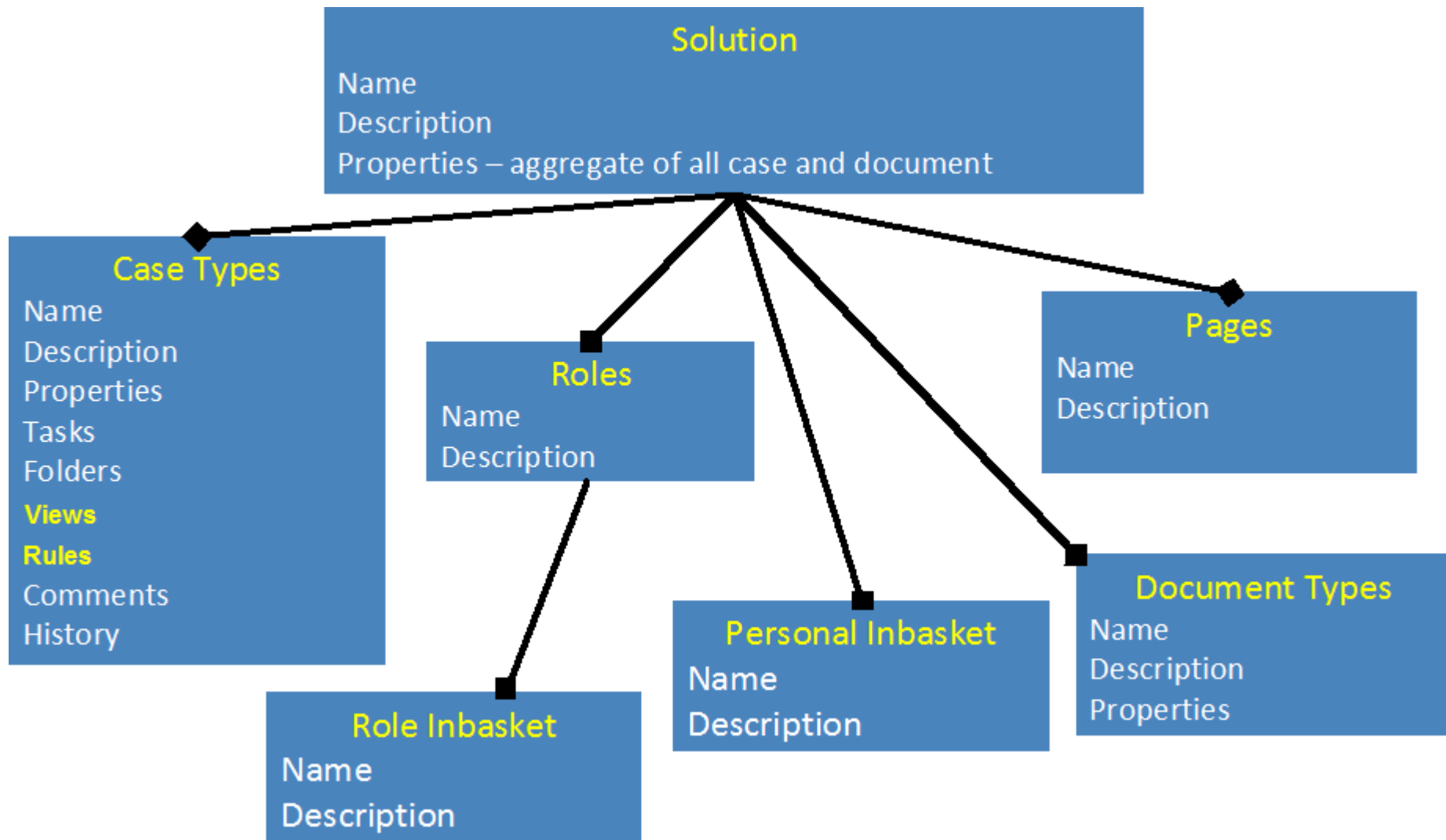
- Process Services Queues, Event Logs, Roster and Application Space

- Additional Security Best Practices

- Q & A



# ICM Solution Model Overview




# ICM Solution and Pages


IBM Case Manager Builder

Intgpeadmin ? IBM

Manage Solutions \ Steven Security Test 3


Show Locked Items Validate Save Save and Close Close




**Steven Security Test 3**  
Steven Security Test 3   
Solution prefix: SST3  
Created by pwtest370  
Created on July 20, 2013


Properties Roles In-baskets Document Types **Pages** Case Types


? Add Page OK All


▼ Solution Pages 


Page Name ^	Description ^
Reports	
Work	View and work with work items in a personal in-basket and the in-basket that i...
Cases	Search for cases, view a list of results, and view a summary of the case p...


► Case Details Pages 

► Add Case Pages 

► Split Case Pages 


► Add Task Pages 

► Work Details Pages 

► Custom Task Pages 

© Copyright IBM Corp. 2013.


10  
– IBM Confidential –



# ICM Solution Pages for a Role


**IBM Case Manager Builder**

Manage Solutions \ **Steven Security Test 3**



**Steven Security Test 3**  
Steven Security Test 3  
Solution prefix: SST3  
Created by pwtest370  
Created on July 20, 2013

PropertiesRolesIn-basketsDocument TypesPagesCase Types

Add RoleOK All

**Partner** outside worker

**Worker** back office worker

\* Role:  
Supervisor

Description:  
back office supervisor

Role SettingsPages

Assign Page

Name	Description
Cases	Search for cases, view...
Work	View and work with wor...
Reports	

# ICM Views, Rules, and Custom Task

The screenshot displays the IBM Case Manager Builder interface. At the top, a black header bar contains the text "IBM Case Manager Builder". Below this is a blue navigation bar with the breadcrumb "Manage Solutions \ Steven Secur... \ case1". A left-hand sidebar lists several options: "Case Type" (selected and highlighted in dark blue), "Properties", "Views", "Case Folders", "Rules", and "Tasks". The main content area is titled "Case Type Attributes" with a question mark icon. It contains the following fields and controls:

- \*Case type name:** A text input field containing "case1".
- \*Case type unique identifier:** A text input field containing "SST3\_" followed by a dropdown menu showing "case1".
- Case type description:** A large, empty text area.
- Starting document type:** A dropdown menu currently showing "<None>".
- ☒ **Enable case workers to create custom tasks**
- Default layout for Custom Task Details page:** A dropdown menu showing "Custom Task Details".
- Default layout for Add Case page:** A dropdown menu showing "Add Case".

# ICM Discretionary Tasks

The screenshot displays the IBM Case Manager Builder interface. The top navigation bar includes the title "IBM Case Manager Builder", the user "Intgpeadmin", and the IBM logo. Below this, a breadcrumb trail shows "Manage Solutions \ Steven Secur... \ case1". Action buttons for "Show Locked Items", "Back", "Validate", "Save", and "Save and Close" are present.

A left-hand sidebar contains a menu with the following items: "Case Type", "Properties", "Views", "Case Folders", "Rules", and "Tasks" (which is currently selected and highlighted in blue).


The main workspace is divided into two sections:

- Optional tasks:** This section contains three task cards:
  - case start:** Features a green play icon, a precondition of "Case Start", and a set of "<None>".
  - task 1:** Features a green play icon, a precondition of "Property expression: b1 = True", and a set of "<None>".
  - task 2:** Features a green play icon, a precondition of "Documents: Any document", and a set of "<None>".
- Discretionary tasks:** This section contains two task cards:
  - discretionary 2:** Features a person icon, a set of "<None>", and no precondition.
  - discretionary 1:** Features a person icon, a set of "<None>", and no precondition.

At the top of the main workspace, there are controls for "Add Task" (with a dropdown arrow), "Manage Sets", and "All tasks". A "View by:" filter is set to "Priority | Set | Name".

# ICM Solution Structure










IBM Case Manager administration client



- ICMDOS05\_cmicmint1vm14
  - IBM Case Manager
    - Audit Configurations
    - Connection Definitions
    - Datasets
    - Page Templates
    - Rule Packages
    - Security Configurations
    - Solution Templates
    - Solutions
      - Steven Security Demo
        - nls
        - Pages
        - Rules
        - Views
        - Steven Security Test 1
        - Steven Security Test 2
        - Steven Security Test 3

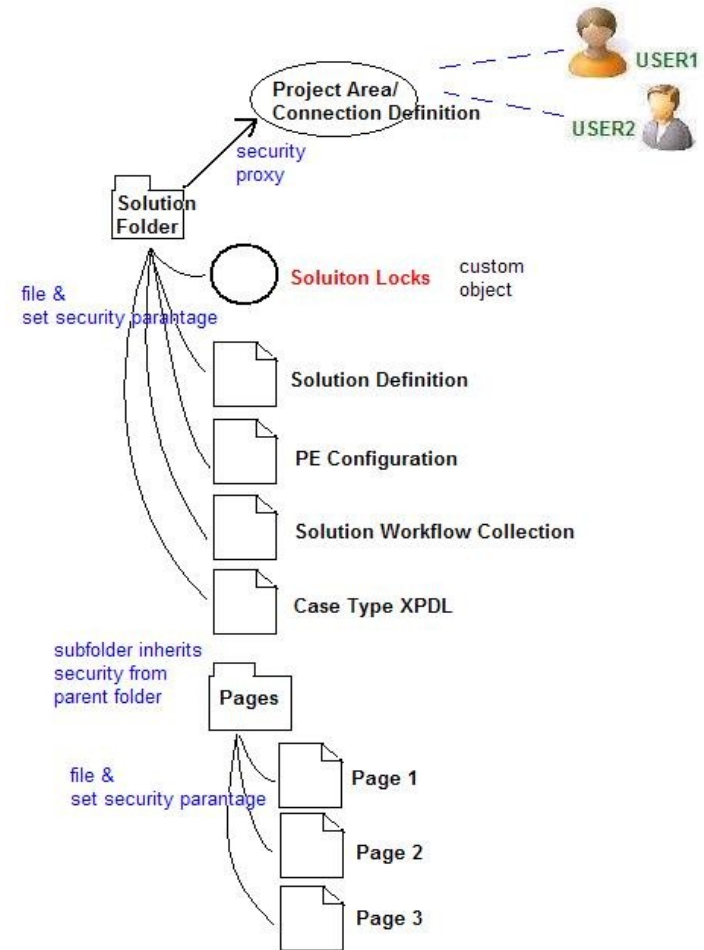
RefreshAdd DocumentNew FolderCheck InCheck OutPropertiesActions ▾

ICMDOS05\_cmicmint1vm14 ▸ IBM Case Manager ▸ Solutions ▸ Steven Security Demo

	Name ▲	Size	Modified By	Modified On
	nls		Intgpeadmin	7/21/2013, 8:43 PM
	Pages		Intgpeadmin	7/21/2013, 8:43 PM
	Rules		Intgpeadmin	7/21/2013, 8:43 PM
	Views		Intgpeadmin	7/21/2013, 8:43 PM
	case1 Workflow Definition	34 KB	Intgpeadmin	7/21/2013, 8:43 PM
	case2 Workflow Definition	1 KB	Intgpeadmin	7/21/2013, 8:43 PM
	PE Configuration	49 KB	Intgpeadmin	7/21/2013, 8:43 PM
	Solution Definition	30 KB	Intgpeadmin	7/21/2013, 8:43 PM
	Solution Workflow Collection	1 KB	Intgpeadmin	7/21/2013, 8:43 PM

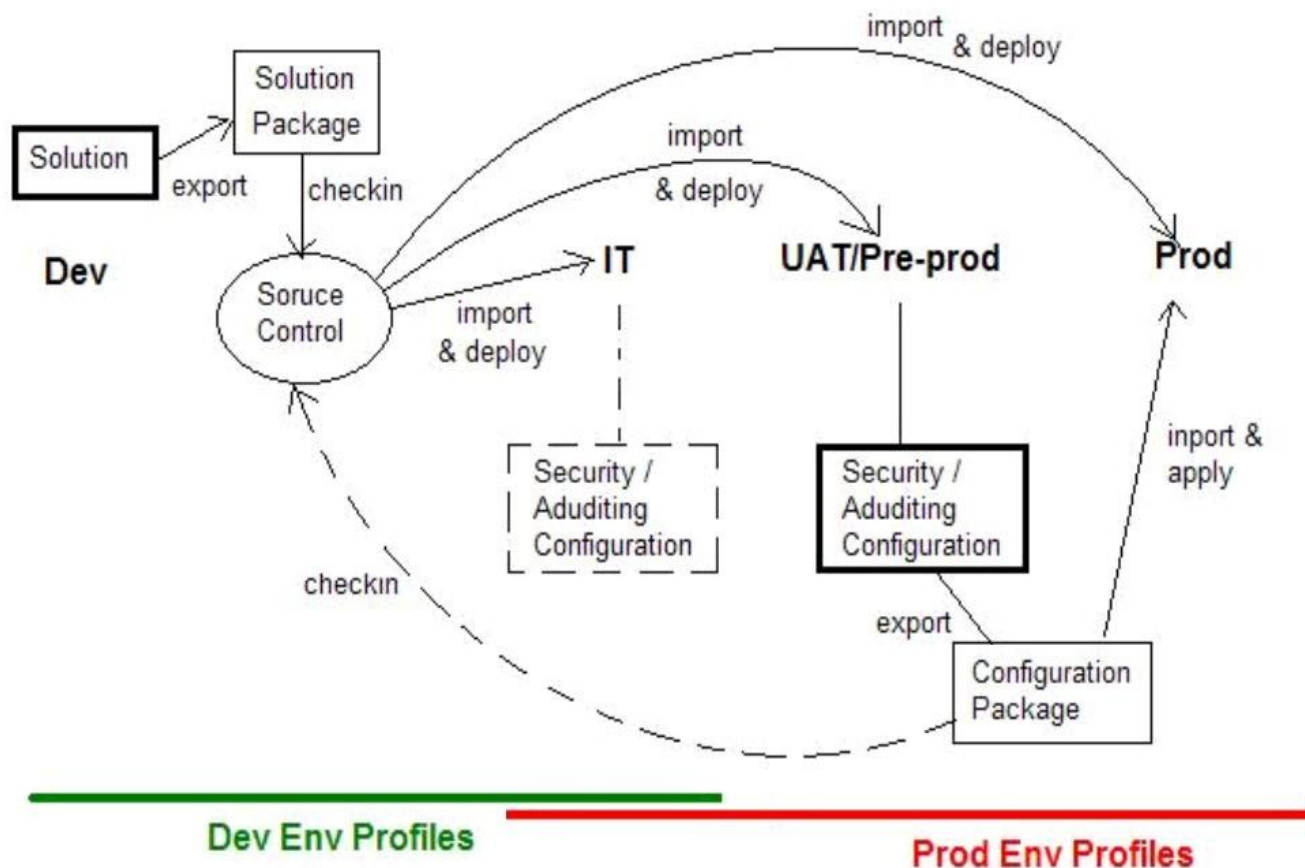
# Design Object Store Security

- IT/ICM Solution Administrator has control over Staging OS
- Treat the Design OS in Development Environment just like a source control system
  - Only groups/users assigned to Project Area has authoring rights to corresponding solutions within the project area
  - Solution security is dynamically reflected
- Remaining sections focus on Target Environment security model



# Stages of Target Environments

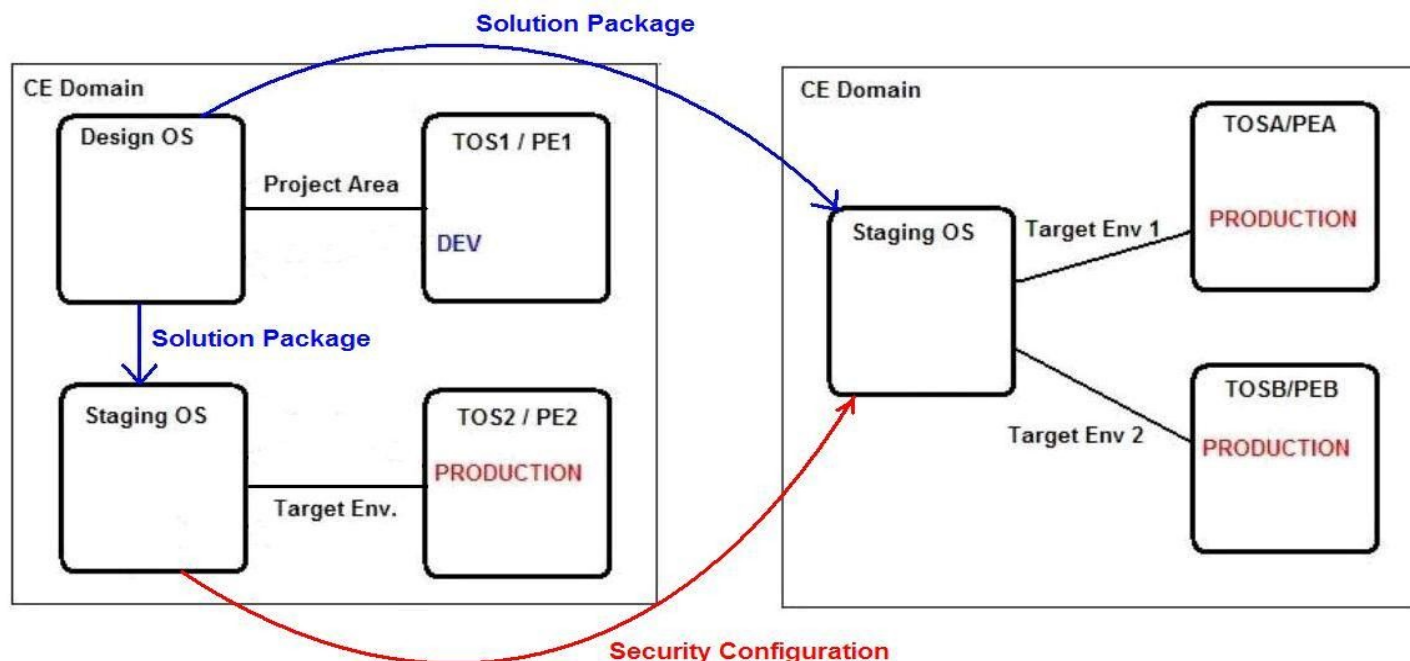
- Solution Package coming from Development Environment
- Security tests are configured/tested early via production environment profile





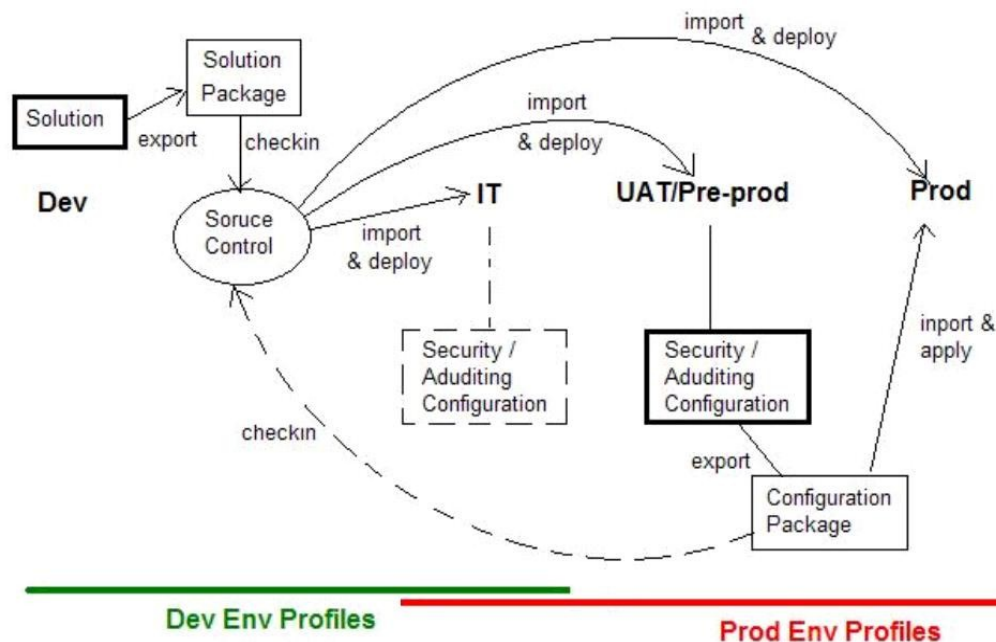
# Target Environment for Security Tests

- Development Environment and Production Environment (IT/UAT) can be within same CE Domain or multiple Domains
- Exercise solution migration properly
- Configure security for a deployed solution as if it is in a production system
  - Do not sign in as administrator into Case Client



# Solution Package vs. Security/Auditing Configuration

- Solution Package may be less updated while Security and Auditing are more frequently changed based on business needs and mandates
  - Different change lifecycle
- Same Solution Package may be delivered and deployed to multiple Geo's Data Centers for a global enterprise, where security access rights and role memberships are maintained and adjusted based on local Directory Services of the Geo



# Call to Action

- Understand customer business requirements as well as security models needed in order to build a good ICM solution
- Design the solution and plan security accordingly
- Prepare proper security test plan, scenario coverages and allocate amount of test time needed to exercise the plan
- No excuse for security not well understood nor tested thoroughly already before going into UAT or PROD, or to a client site

# Session Roadmap

- Target Environment Security Planning and Configuration
- ICM Solution Model and Solution Structure
- Case Manager Security Model
- Deployed Solutions and Case Client
- Content Engine Classes and Objects
- Process Services Queues, Event Logs, Roster and Application Space
- Additional Security Best Practices
- Q & A

# Content Engine Create Instance Rights

- Class Definition controls
  - Who can view the class
  - Who can create an instance of the class

The screenshot displays the IBM Administrative Console for Content Engine. The left sidebar shows a tree view of the object store, with 'TOS05\_cmimint1vm14' selected. The main area shows the 'case1' class definition. The 'Security' tab is active, displaying a table of users and groups with checkboxes for permissions. The 'Edit Permissions' dialog is open, showing the 'Users and Groups' list with 'pwtest350' selected. The 'Permission type' is set to 'Allow', 'Apply to' is 'This object only', and 'Permission group' is 'Custom'. The 'View all properties' checkbox is checked, and the 'Create instance' checkbox is also checked. The 'Owner' field is visible at the bottom of the dialog.

IBM Administrative Console for Content Engine

Object Store: TOS05\_cmimint1vm14

Class Definition: case1

Security Policy

You can allow or deny permissions to a user or group. Each permission group contains one or more access rights.

Predefined permissions are collections of permissions. You can select one or more predefined permissions to apply to the selected object.

**Edit Permissions**

Users and Groups:

Name
Intgpeadmin
<input checked="" type="checkbox"/> pwtest350
<input type="checkbox"/> pwtest351
<input type="checkbox"/> pwtestadmin

Permission type: Allow

Apply to: This object only

Permission group: Custom

☒ View all properties

☐ Link

☐ Create subclass

☒ Read permissions

☐ Modify owner

☐ Modify all properties

☒ Create instance

☐ Delete

☐ Modify permissions

Owner: ?

Change Owner

OK Cancel

# Content Engine Create Instance Rights (cont)

- Case Type
  - Solution Case Types are subclasses of Case Folder
  - Also needs Deployed Case Type folder side security
- Case Subfolder
  - No subclasses, all OS users can create case subfolder
  - Also needs Create Subfolder right on case or case subfolder
- Document Type
  - Solution Document Types are subclasses of Document Class
  - Also needs File in Folder right on the case or case subfolder
- Discretionary Task Types
  - Solution Task Types are subclasses of Case Task
  - Also needs Process Services Roster create right
- Dynamic Task
  - There is one subclass for each Case Type enabled for Dynamic Task
  - Also needs Process Services Roster create right
- Comments
  - All OS users can create comments
  - Also needs Annotate right on the case

# Production Environment Profile

- The Configuration Tool empties out Default Instance Security settings from various ICM AddOn base classes if it is an production environment profile
- Case Folder, Case Subfolder, Case Type Subfolder

The screenshot displays the IBM Administrative Console for Content Engine. The left sidebar shows a tree view of the object store structure, with 'Case Folder' selected under 'Classes'. The main panel shows the 'Default Instance Security' tab for the 'Case Folder' class. The tab includes a 'Users and Groups' section with an 'Add...' button and a table with columns: Name, Source, Permission Type, Permission Group, and Apply To. The table is currently empty, displaying 'No content available.'.

IBM Administrative Console for Content Engine

Object Store: TOS05\_cmicmint1vm14

Class Definition: Case Folder

Default Instance Security

You can allow or deny permissions to a user or group. Each permission group contains one or more access rights.

Predefined permissions are collections of access rights that grant varying degrees of access to the object. When you select a predefined permission group, the permission group are selected. You can customize a predefined permission as needed. [Learn more...](#)

Users and Groups

Add... Edit... Remove

0 total Filter by n

		Name	Source	Permission Type	Permission Group	Apply To
No content available.						

# Production Environment Profile (cont.)

- Case Task
  - Dynamic Task
  - Task With Initiating Document (deprecated)

The screenshot displays the IBM Administrative Console for Content Engine. The left sidebar shows a tree view of the object store structure, with 'Task' and 'Case Task' selected. The main panel shows the 'Case Task' configuration page, which includes tabs for 'General', 'Properties', 'Property Definitions', 'Default Instance Security', 'Security', and 'Change Preprocess'. The 'Default Instance Security' tab is active, showing a table for 'Users and Groups' with columns for 'Name', 'Source', 'Permission Type', 'Permission Group', and 'Appl'. The table is currently empty, displaying 'No content available.'

IBM Administrative Console for Content Engine

Object Store: TOS05\_cmicmint1vm14

TOS05\_cmicmint1vm14

- Administrative
- Browse
- Data Design
  - Choice Lists
  - Classes
    - Custom Object
    - Document
    - Folder
    - Other Classes
- Task
  - Case Task**
    - Dynamic Task
    - Task With Initiating Document
  - Task Relationship
  - Text Search Index Request
  - Thumbnail
  - Version Series
- Property Templates

Class Definition: Case Task

Save Refresh Actions Close

General Properties Property Definitions **Default Instance Security** Security Change Preprocess

You can allow or deny permissions to a user or group. Each permission group contains one or more access rights.

Predefined permissions are collections of access rights that grant varying degrees of access to the object. When you select a predefined permission that are included in the permission group are selected. You can customize a predefined permission as needed. [Learn more...](#)

Users and Groups

Add... Edit... Remove 0 total Filter by name

		Name	Source	Permission Type	Permission Group	Appl
No content available.						



# Production Environment Profile (cont.)

- Case Comment, Task Comment, Work Item Comment, and Version Series Comment with #CREATOR\_OWNER only

The screenshot displays the IBM Administrative Console for Content Engine. The left sidebar shows a tree view of the object store structure, with 'Case Comment' selected under 'Other Classes'. The main panel shows the 'Class Definition: Case Comment' configuration. The 'Default Instance Security' tab is active, showing a table of predefined permissions. The table lists one permission: '#CREATOR-OWNER' with a 'Direct' source, 'Allow' permission type, 'Full Control' permission group, and 'Apply To: This object only'.

IBM Administrative Console for Content Engine

Object Store: TOS05\_cmictim1vm14

Class Definition: Case Comment

Default Instance Security

You can allow or deny permissions to a user or group. Each permission group contains one or more access rights.

Predefined permissions are collections of access rights that grant varying degrees of access to the object. When you select a predefined permission group that are included in the permission group are selected. You can customize a predefined permission as needed. [Learn more...](#)

Users and Groups

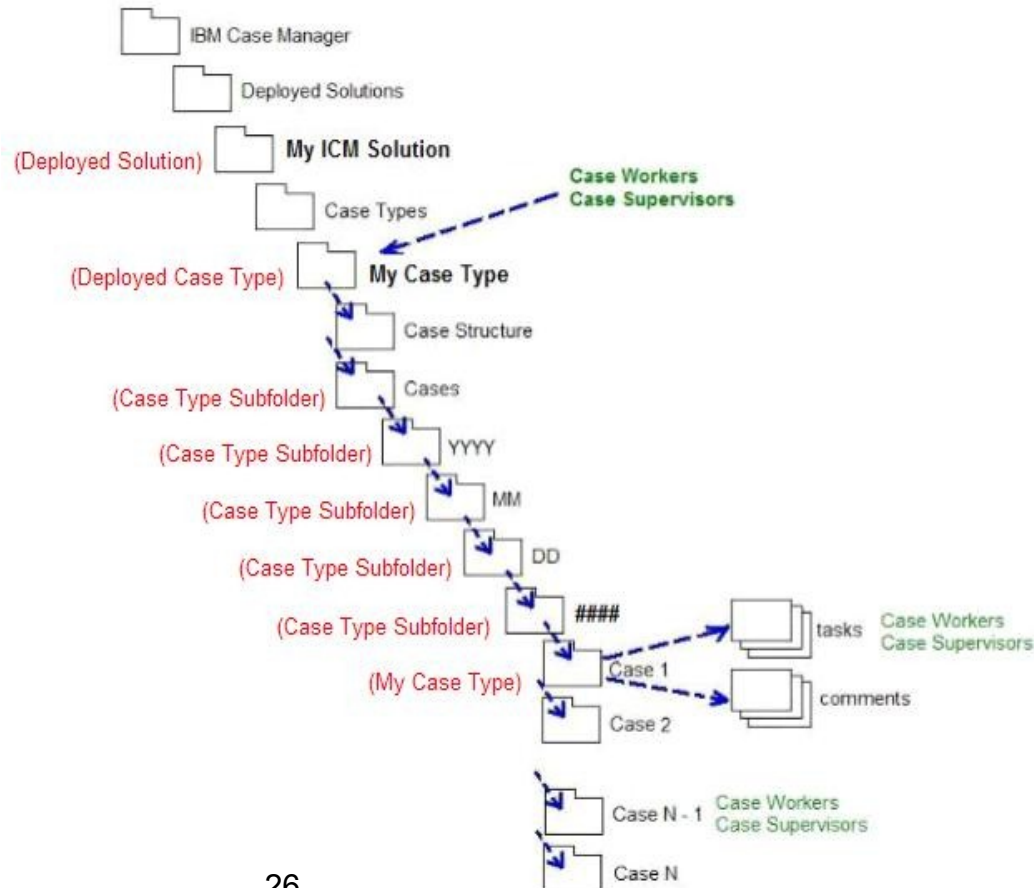
1 total

Filter by name

	Name	Source	Permission Type	Permission Group	Apply To
<input type="checkbox"/>	#CREATOR-OWNER	Direct	Allow	Full Control	This object only

# Dynamic Security Inheritance Model

- ICM recommends and uses dynamic security inheritance model
  - Not using default instance security allows the security to be configured at the Deployed Case Type folder level, and inherited cleanly all the way down

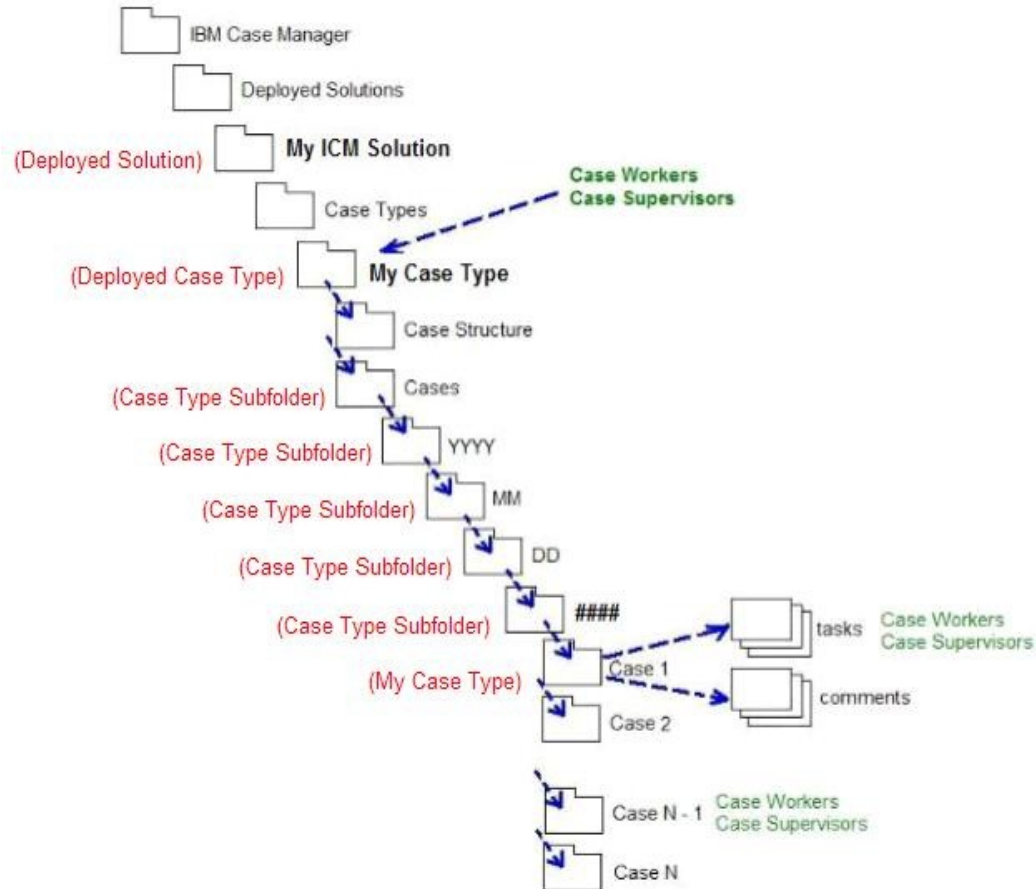


## Dynamic Security Inheritance Model (cont.)

- Using Default Instance Security adds ACEs into object instance directly
  - Future update/change of the security across all existing instances could become very difficult
    - Need extra program or script to search for existing case instances, and do update by batch as well as good recovery/retry instrumentation to ensure system integrity
- Dynamic Security Inheritance allows changes of security easily that can be triggered by any personnel functional responsibility change, corporate structural reorganization, business model/requirement update, or government mandates, etc.
  - Only a fixed number of well-known control points need security update and let the platform reflects the security change dynamically & reliably

# Dynamic Security Inheritance Model (cont.)

- The default model assumes all case instances has same rights following the deployed case type folder
  - Variations of instance based security model discussed later



# Document Security Model

- Existing document classes may be reused into an ICM solution
  - Already has default security configuration settings to be used as is
- Document can be shared (multi-filed) across cases
  - When a document is filed into different cases, its security in general should not be changed as a side-effect in order to avoid unexpected security concern or issue
    - e.g. a document a user can only see and not able to modify its properties, nor authoring – i.e. checkout/checkin, its security should not be altered even if the user files that document into a case which the user has more elevated rights on the case (like update case properties, modify permission, delete case, etc.)
  - Split case can also cause some documents to be filed into the newly split case of same or different Case Type
    - A different Case Type may have different security
- Generally document security needs careful planning and review, and it can be highly diverse from customer to customer business scenarios

# Document Security Model (cont.)

- In Case Manager, case documents still use the standard default instance security model controlled by document subclasses
  - A custom variation of case owned document (never filed to another case) is discussed later

The screenshot displays the IBM Administrative Console for Content Engine. The left sidebar shows a tree view of the 'TOS05\_cmimint1vm14' object store, with 'Classes' > 'Document' > 'doc1' selected. The main panel shows the 'Class Definition: doc1' configuration. The 'Default Instance Security' tab is active, showing a table of permissions for 'doc1'.

Object Store: TOS05\_cmimint1vm14

Class Definition: doc1

Permissions:

	Name	Source	Permission Type	Permission Group	Apply To
<input checked="" type="checkbox"/>	intg_admin	Direct	Allow	Full Control	This object only
<input type="checkbox"/>	intg_test	Direct	Allow	View content	This object only
<input type="checkbox"/>	WCM Administrators	Direct	Allow	Full Control	This object only
<input type="checkbox"/>	WCM Editors	Direct	Allow	View content	This object only
<input type="checkbox"/>	WcmTestG4	Direct	Allow	Full Control	This object only

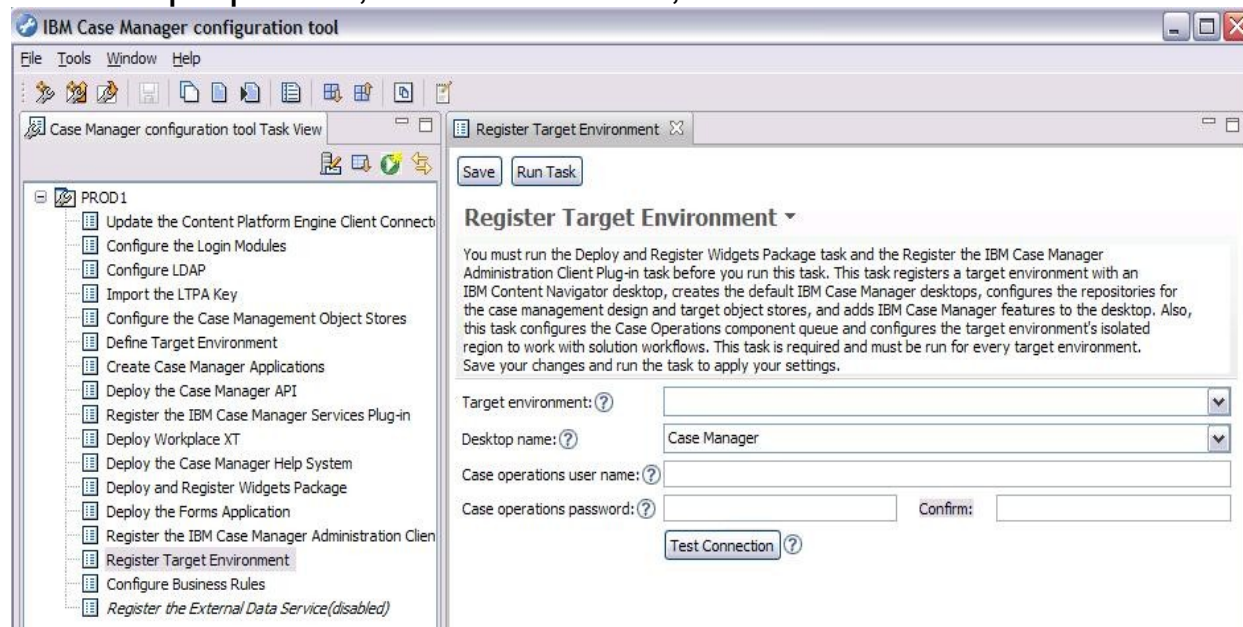
# Process Services Security Model

- Do not leave Process Services security open
  - Only secured on CE side is not sufficient
- Setup Process Services Administrator and Configuration groups to IT/ICM Solution Administrators
- Application Space (for the solution)
  - Users that can manage roles need to be added into Application Space security
  - No longer needs to be adjusted for Reassign Work to see all roles
- Roster (for the solution)
  - Controls task process creation/launching
  - Users who might start a task, e.g. during case creation, create and start a discretionary or custom task, etc. will need Create right
- Event Log (for each case type) – used by Case History/Visualizer
- Work Queue (for each role)
  - Query and Process rights to get to work object and process/dispatch
  - CE side security further influenced by the task processes design as well
  - User who can view/query the work items, select a response and influence how the work is routed next ... but can only view case
    - i.e. does not update case property, nor add document, etc.
  - User who can actually update the work item (case properties exposed on the step UI as R/W) with new values, add document, create comment, etc.



# Component Queue Workers

- Configuration Tool configures the default ICM OOTB component queues security
  - Case Operations, Rule Operations
  - Do not use CPE Administrator account, customer typically uses a delegated non-FullControl account instead
  - This non-UI worker/account designated also needs Content Engine side security configuration in order to perform the operations, e.g. create a case, update case properties, file a document, etc.





# Component Queue Workers (cont.)

- Customer IT/ICM Solution Administrators further need to take care of CE Operations queue as well as any additional custom component queue(s) security configuration accordingly

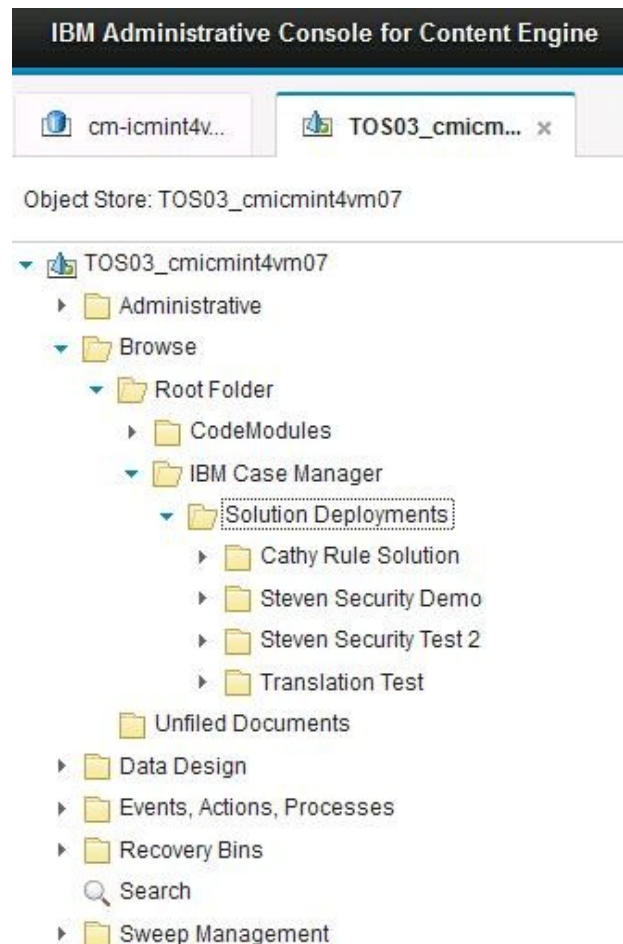
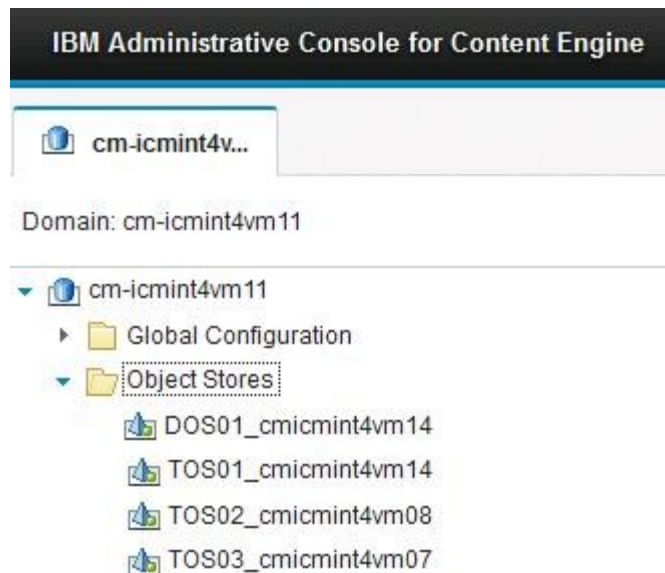
The screenshot displays the IBM Administrative Console for Content Engine. The left sidebar shows a tree view of the system configuration, with 'TOS05\_cmimint1vm14' selected. The main pane shows the 'Component Properties' dialog for the 'TOS05\_cmimint1vm14\_500' configuration. The 'Adapter' tab is active, showing the 'Adapter' dropdown set to 'Java Component'. The 'Adapter Properties' section includes fields for 'Batch Size' (10), 'Polling Rate (ms)' (1000), 'Exception Submap' (Malfunction), 'Processing Timeout (ms)' (30000), 'Auto Recovery Timeout' (20), and 'Minute(s)' (dropdown). The 'Number of Dispatcher Tasks' is set to 1, and the 'Enable Queue Processing In Server' checkbox is checked. The 'JAAS Credentials' section shows 'User Name' as 'intgpeadmin' and 'Password' as masked. The 'Configuration Context' field is empty.

# Session Roadmap

- Target Environment Security Planning and Configuration
- ICM Solution Model and Solution Structure
- Case Manager Security Model
- Deployed Solutions and Case Client
- Content Engine Classes and Objects
- Process Services Queues, Event Logs, Roster and Application Space
- Additional Security Best Practices
- Q & A

# Target Environment and Deployed Solutions

- A CE Domain can have multiple target object stores
- Each target object stores can have multiple deployed solutions



# Security Configuration for a Deployed Solution

- Grant groups/users with “view” rights to a deployed solution folder to allow access, i.e. see and use the solution

The screenshot displays the IBM Administrative Console for Content Engine. The left sidebar shows a tree view of the object store 'TOS03\_cmimint4vm07', with the 'Steven Security Demo' folder selected under 'Solution Deployments'. The main panel shows the 'Security' tab for this folder. It includes a 'Users and Groups' section with a table of users and their permissions.

Object Store: TOS03\_cmimint4vm07

Folder: Steven Security Demo

Security Policy

You can allow or deny permissions to a user or group. Each permission group contains one or more access rights. Predefined permissions are collections of access rights that grant varying degrees of access to the object. When you select a predefined permission group, the access rights that are included in the permission group are selected. You can customize a predefined permission as needed. [Learn more...](#)

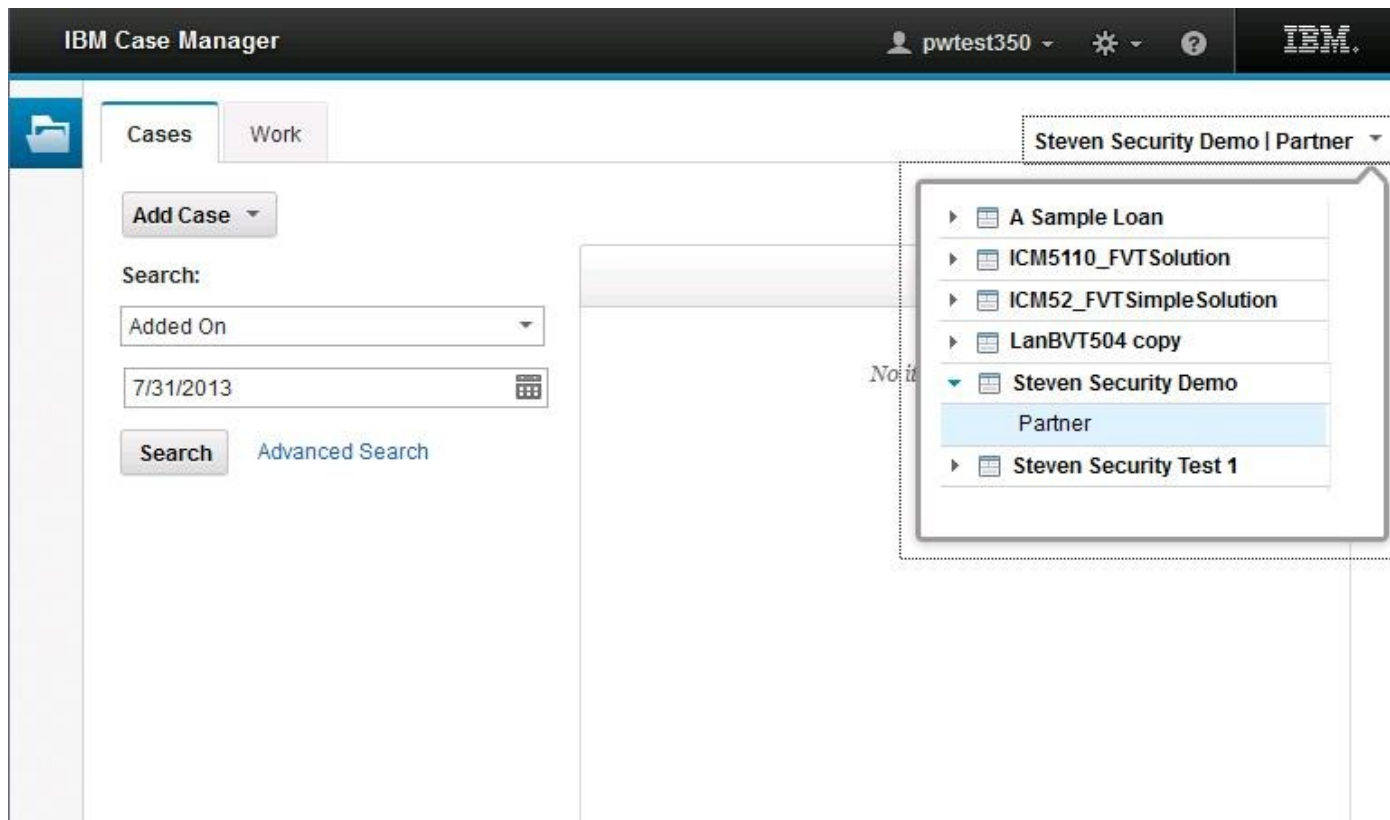
Users and Groups

12 total

	Name	Source	Permission Type	Permission Group	Apply To
<input type="checkbox"/>	Intgpeadmin@langley.local	Direct	Allow	Full Control	This object and all children
<input type="checkbox"/>	pwtest320@langley.local	Direct	Allow	Custom	This object only
<input type="checkbox"/>	pwtest350@langley.local	Direct	Allow	Custom	This object only
<input type="checkbox"/>	pwtest351@langley.local	Direct	Allow	Custom	This object only
<input type="checkbox"/>	pwtest360@langley.local	Direct	Allow	Custom	This object only

# Deployed Solutions and Case Client

- When a user signs into Case Client, the user can access all the solutions deployed within the CE domain that the user has “view” rights to
  - i.e. the deployed solutions available for a user are discovered and collected from multiple target object stores

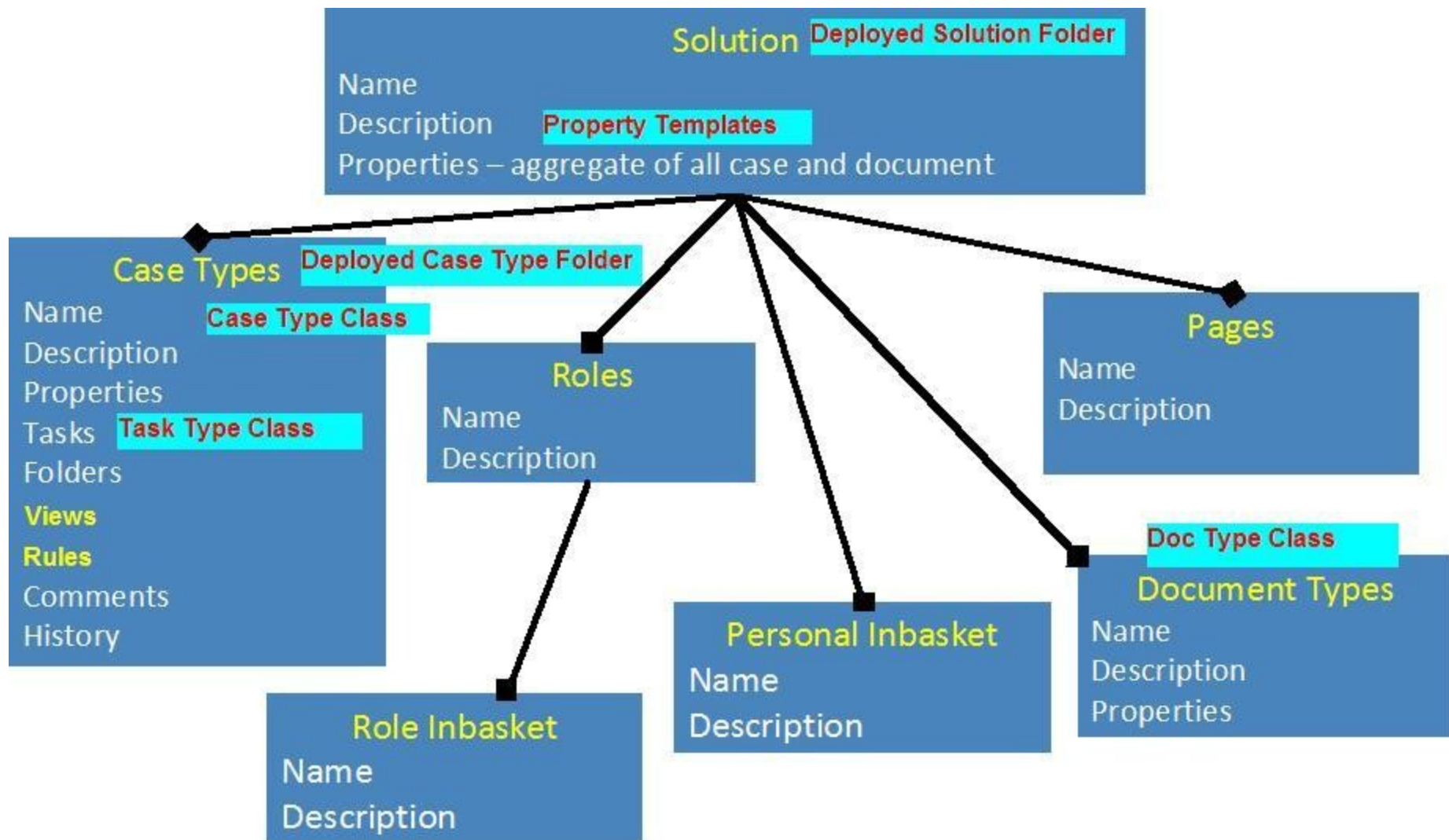


# Session Roadmap

- Target Environment Security Planning and Configuration
- ICM Solution Model and Solution Structure
- Case Manager Security Model
- Deployed Solutions and Case Client
- ➔Content Engine Classes and Objects
- Process Services Queues, Event Logs, Roster and Application Space
- Additional Security Best Practices
- Q & A



# ICM Solution Model to CE Classes and Objects



# Case Type Classes

- Solution Case Types are subclasses of Case Folder class

The screenshot displays the IBM Administrative Console for Content Engine. The left sidebar shows a tree view of the object store 'TOS05\_cmimint1vm14', with 'Case Folder' selected under 'Classes'. The main area shows the 'Class Definition: case1' with tabs for General, Properties, Property Definitions, Default Instance Security, Security Policy, Security, and Retention. The 'Security' tab is active, showing a list of 'Users and Groups' with checkboxes for permissions. An 'Edit Permissions' dialog is open, showing a table of users and groups, and a list of permissions to be applied to 'pwtest350'.

IBM Administrative Console for Content Engine

Object Store: TOS05\_cmimint1vm14

Class Definition: case1

Security

You can allow or deny permissions to a user or group. Each permission group contains one or more access rights.

Predefined permissions are collections of permissions. You can select one or more predefined permissions in the permission group are selected. You can also create a custom permission group.

**Edit Permissions**

Users and Groups:

✓	Name
<input type="checkbox"/>	Intgpeadmin
<input checked="" type="checkbox"/>	pwtest350
<input type="checkbox"/>	pwtest351
<input type="checkbox"/>	pwtestadmin

Permission type: Allow

Apply to: This object only

Permission group: Custom

☒ View all properties ☐ Modify all properties

☐ Link ☒ Create instance

☐ Create subclass ☐ Delete

☒ Read permissions ☐ Modify permissions

☐ Modify owner

OK Cancel



# Case Type Classes (cont.)

- Case Type Class Definition controls
  - who can see a Case Type
  - who can create a case instance off the Case Type

The screenshot displays the IBM Case Manager web application interface. At the top, a dark navigation bar contains the text 'IBM Case Manager', a user profile icon labeled 'pwtest350', a settings gear icon, a help question mark icon, and the IBM logo. Below this, a secondary navigation bar features tabs for 'Cases' and 'Work', with 'Work' being the active tab. To the right of the tabs, it says 'Steven Security Demo | Partner' with a dropdown arrow. A 'Manage Roles' button is visible on the left. A 'Partner (0)' button is also present. A dashed box highlights an 'Add Case' dropdown menu, which is open and shows two options: 'case1' and 'case2'. Below the navigation area, there is a filter bar that says 'Filter: No filters applied' with a 'Reset' link. Underneath the filter bar is a table with the following headers: 'Step Name', 'Time Created', and 'Subject'. The table body is empty, and a message 'The in-basket is empty' is displayed in the center.

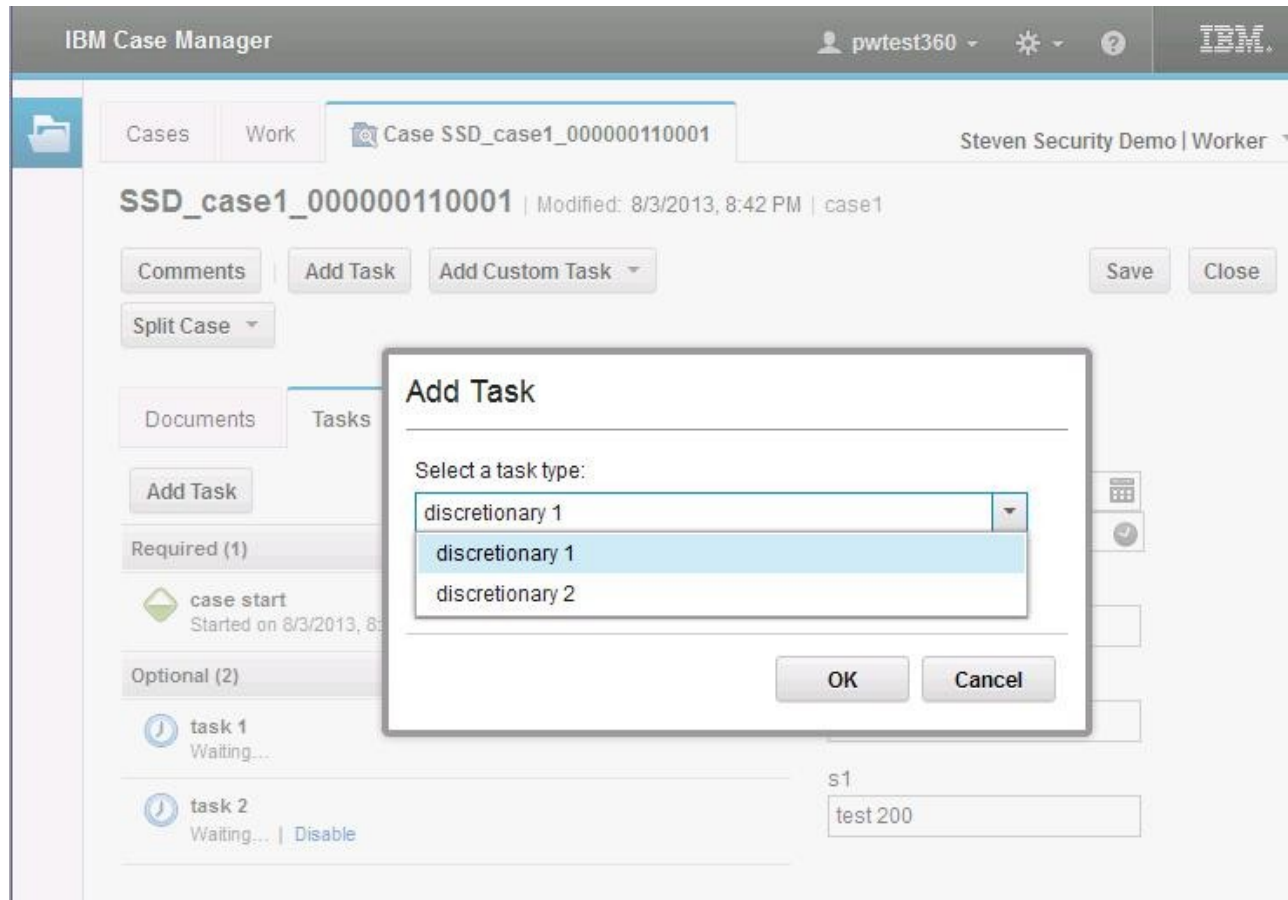
# Discretionary Task Type Classes

- Discretionary Task Types are subclasses of Case Task class

The screenshot displays the IBM Administrative Console for Content Engine. The left sidebar shows a tree view of the object store 'TOS05\_cmimint1vm14', with 'discretionary 1' selected under the 'Task' category. The main panel shows the 'Class Definition: discretionary 1' configuration. The 'Security' tab is active, displaying the 'Edit Permissions' dialog. In this dialog, the 'Users and Groups' list includes 'pwtest360'. The 'Permission type' is set to 'Allow', 'Apply to' is 'This object only', and 'Permission group' is 'Custom'. The 'View all properties' and 'Read permissions' checkboxes are checked. The 'Owner' field is visible at the bottom of the dialog.

# Discretionary Task Type Classes (cont.)

- Discretionary Task Type Class Definition controls
  - who can see and create a task instance off the Discretionary Task Type



# Dynamic Task Type Classes

- Dynamic Task Type of a Case Type is a subclass of Dynamic Task class

The screenshot displays the IBM Administrative Console for Content Engine. The left sidebar shows a tree view of the object store 'TOS05\_cmicmint1vm14', with 'case1 Dynamic Task' selected under 'Dynamic Task'. The main panel shows the 'Class Definition: case1 Dynamic Task' with tabs for General, Properties, Property Definitions, Default Instance Security, and Security. The Security tab is active, showing the 'Edit Permissions' section. A table lists 'Users and Groups' with columns for Name, Image, and Inherited. The 'pwtest360' user is selected. Below the table, the 'Permission type' is set to 'Allow', 'Apply to' is 'This object only', and 'Permission group' is 'Custom'. A list of permissions is shown with checkboxes: View all properties, Link, Create subclass, Read permissions, Modify owner, Modify all properties, Create instance, Delete, and Modify permissions.

IBM Administrative Console for Content Engine

Object Store: TOS05\_cmicmint1vm14

Class Definition: case1 Dynamic Task

Security

You can allow or deny permissions to a user or group. Each permission group contains one or more access rights.

Predefined permission group, the needed. [Learn more...](#)

**Edit Permissions**

Users and Groups:

Name	Image	Inherited
pwtest360		
pwtest360		
pwtest360		
pwtest360		
pwtest360		

Permission type: Allow

Apply to: This object only

Permission group: Custom

☒ View all properties ☐ Link ☐ Create subclass ☒ Read permissions ☐ Modify owner

☐ Modify all properties ☒ Create instance ☐ Delete ☐ Modify permissions

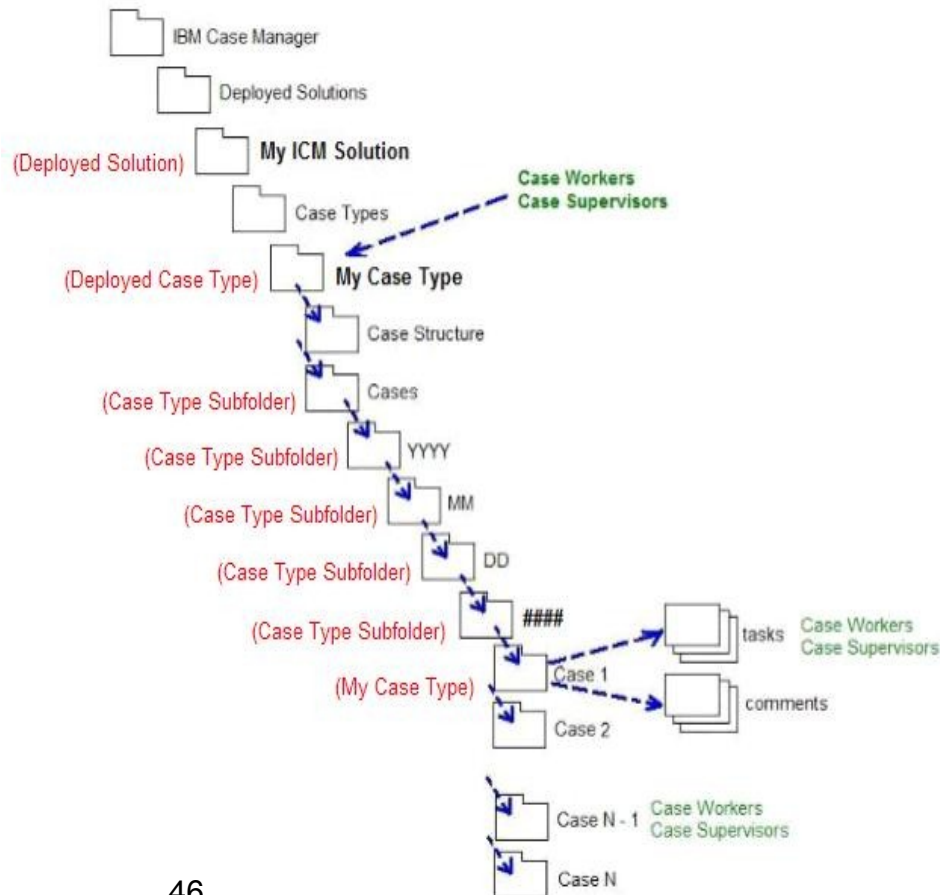
# Dynamic Task Type Classes (cont.)

- Dynamic Task Type Class Definition controls
  - who can define/create a custom task for a case in Case Client during runtime

The screenshot displays the IBM Case Manager web application. At the top, the header shows 'IBM Case Manager' and a user profile 'pwtest360'. The main navigation bar includes 'Cases' and 'Work' tabs. The current case is 'Case SSD\_case1\_000000110001', modified on 8/3/2013 at 8:42 PM. The user is 'Steven Security Demo | Worker'. The 'Add Custom Task' dropdown menu is open, showing 'New' and 'Copy Existing' options. The 'Custom Task Editor' is open, showing a task titled 'My Custom Task' with the description 'this is a custom task demo'. Below the task description, there is a section for 'Work items for this task' with one item: '1 get W2' assigned to 'Worker'. The interface includes various toolbars for editing and managing the task.

# Deployed Case Type Folder

- Deployed Case Type Folder controls a lot of Case Client UI operations
- Each Case Type class has a corresponding Deployed Case Type Folder
  - By default, the deployed case type folder instance has no security set



# Deployed Case Type Folder (cont.)

The screenshot displays the IBM Administrative Console for Content Engine. The left sidebar shows a tree view of the object store 'TOS05\_cmicmint1vm14', with the 'SSD\_case1' folder selected under 'Case Types'. The main panel shows the 'SSD\_case1' folder details, including tabs for 'Contents', 'General', 'Properties', 'Annotations', 'Security Policy', 'Security', 'Retention', and 'Transfer'. The 'Security' tab is active, showing a table of users and groups with checkboxes for permissions. An 'Edit Permissions' dialog is open, showing the 'Users and Groups' list with 'pwtest360' selected. The dialog also shows the 'Permission type' (Allow), 'Apply to' (This object and all children), and 'Permission group' (Custom). The 'Permission group' section contains two columns of checkboxes for various permissions, including 'View all properties', 'Modify all properties', 'File in folder / Annotate', 'Unfile from folder', 'Create instance', 'Create subfolder', 'Delete', 'Read permissions', 'Reserved12 (Deploy is deprecated)', 'Reserved13 (Archive is deprecated)', 'Modify permissions', and 'Modify owner'.

IBM Administrative Console for Content Engine

Object Store: TOS05\_cmicmint1vm14

Folder: SSD\_case1

Security Policy

Security

Retention

Transfer

You can allow or deny permission for this folder and its contents. Predefined permissions are collected into permission groups, the access rights needed. [Learn more...](#)

Users and Groups

	Name
<input checked="" type="checkbox"/>	pwtest360
<input type="checkbox"/>	pwtest361
<input type="checkbox"/>	pwtest362
<input type="checkbox"/>	pwtest370
<input type="checkbox"/>	pwtest380

Owner/Active Markings

Change Owner

Permission type: Allow

Apply to: This object and all children

Permission group: Custom

<input checked="" type="checkbox"/> View all properties	<input checked="" type="checkbox"/> Modify all properties
<input type="checkbox"/> Reserved12 (Deploy is deprecated)	<input type="checkbox"/> Reserved13 (Archive is deprecated)
<input checked="" type="checkbox"/> File in folder / Annotate	<input checked="" type="checkbox"/> Unfile from folder
<input type="checkbox"/> Create instance	<input checked="" type="checkbox"/> Create subfolder
<input type="checkbox"/> Delete	<input checked="" type="checkbox"/> Read permissions
<input type="checkbox"/> Modify permissions	<input type="checkbox"/> Modify owner

OK Cancel



## Deployed Case Type Folder (cont.)

- View Case, Case Subfolders, Tasks, Comments, Case History, etc.

The screenshot shows the 'Edit Permissions' dialog box. At the top, the title is 'Edit Permissions'. Below it, there is a section for 'Users and Groups' with a text box containing 'pwtest370'. Underneath, there are three dropdown menus: 'Permission type' set to 'Allow', 'Apply to' set to 'This object and all children', and 'Permission group' set to 'View properties'. Below these are two columns of checkboxes. The first column includes: 'View all properties' (checked), 'Reserved12 (Deploy is deprecated)' (unchecked), 'File in folder / Annotate' (unchecked), 'Create instance' (unchecked), 'Delete' (unchecked), and 'Modify permissions' (unchecked). The second column includes: 'Modify all properties' (unchecked), 'Reserved13 (Archive is deprecated)' (unchecked), 'Unfile from folder' (unchecked), 'Create subfolder' (unchecked), 'Read permissions' (checked), and 'Modify owner' (unchecked). At the bottom right, there are 'OK' and 'Cancel' buttons.



## Deployed Case Type Folder (cont.)

- Unless a user has view right on the case, the case will not even be returned in Cases search
  - In turn user will not get into Case Detail Page



IBM Case Manager

pwtest360

Steven Security Demo | Worker

Cases Work

Add Case

Search: Case Identifier

%

Search Advanced Search

Title	Case Identifier	Case Type	Case State
SSD_case1_000000110001	SSD_case1_000000110001	case1	Working

SSD\_case1\_000000110001

Summary History

b1: false

dt1: No value

f1: 200

i1: 200

s1: test 200



IBM Case Manager

pwtest350

Steven Security Demo | Partner

Cases Work

Add Case

Search: Case Identifier

%

Search Advanced Search

Title	Case Identifier	Case Type	Case State
SSD_case1_000000110001	SSD_case1_000000110001	case1	Working
SSD_case1_000000110001	SSD_case1_000000110001	case1	Working

SSD\_case1\_000000110001

Summary History

b1: true

dt1: No value

f1: 100

i1: 100

s1: test 100

## Deployed Case Type Folder (cont.)

- Update Case Properties, Task Properties and States, etc.

**Edit Permissions**

Users and Groups: pwtest370

Permission type: Allow

Apply to: This object and all children

Permission group: Custom

<input type="checkbox"/> View all properties	<input checked="" type="checkbox"/> Modify all properties
<input type="checkbox"/> Reserved12 (Deploy is deprecated)	<input type="checkbox"/> Reserved13 (Archive is deprecated)
<input type="checkbox"/> File in folder / Annotate	<input type="checkbox"/> Unfile from folder
<input type="checkbox"/> Create instance	<input type="checkbox"/> Create subfolder
<input type="checkbox"/> Delete	<input type="checkbox"/> Read permissions
<input type="checkbox"/> Modify permissions	<input type="checkbox"/> Modify owner

OK Cancel

**Edit Permissions**

Users and Groups: pwtest360  
pwtest370

Permission type: Allow

Apply to: This object and all children

Permission group: Change state

- Full Control
- Modify properties
- Add to Folder
- View properties
- Minor versioning
- Major versioning
- View content
- Change state**
- Publish
- Custom

## Deployed Case Type Folder (cont.)

- Add/File Case Document, Add comment
- Unfile Case Document

The screenshot shows the 'Edit Permissions' dialog box. At the top, the title is 'Edit Permissions'. Below it, there is a section for 'Users and Groups' with a text box containing 'pwtest370'. Underneath, there are three dropdown menus: 'Permission type' set to 'Allow', 'Apply to' set to 'This object and all children', and 'Permission group' set to 'Custom'. Below these are two columns of checkboxes. The left column includes: 'View all properties', 'Reserved12 (Deploy is deprecated)', 'File in folder / Annotate' (checked), 'Create instance', 'Delete', and 'Modify permissions'. The right column includes: 'Modify all properties', 'Reserved13 (Archive is deprecated)', 'Unfile from folder' (checked), 'Create subfolder', 'Read permissions', and 'Modify owner'. At the bottom right, there are 'OK' and 'Cancel' buttons.

## Deployed Case Type Folder (cont.)

- Create Case Subfolder

**Edit Permissions**

Users and Groups: pwtest370

Permission type: Allow

Apply to: This object and all children

Permission group: Custom

<input type="checkbox"/> View all properties	<input type="checkbox"/> Modify all properties
<input type="checkbox"/> Reserved12 (Deploy is deprecated)	<input type="checkbox"/> Reserved13 (Archive is deprecated)
<input type="checkbox"/> File in folder / Annotate	<input type="checkbox"/> Unfile from folder
<input type="checkbox"/> Create instance	<input checked="" type="checkbox"/> Create subfolder
<input type="checkbox"/> Delete	<input type="checkbox"/> Read permissions
<input type="checkbox"/> Modify permissions	<input type="checkbox"/> Modify owner

OK Cancel

## Deployed Case Type Folder (cont.)

- Give additional Modify Permissions, Modify Owner or Delete case assets rights to case supervisors or managers only

**Edit Permissions**

Users and Groups:

Permission type:

Apply to:

Permission group:

<input type="checkbox"/> View all properties	<input type="checkbox"/> Modify all properties
<input type="checkbox"/> Reserved12 (Deploy is deprecated)	<input type="checkbox"/> Reserved13 (Archive is deprecated)
<input type="checkbox"/> File in folder / Annotate	<input type="checkbox"/> Unfile from folder
<input type="checkbox"/> Create instance	<input type="checkbox"/> Create subfolder
<input checked="" type="checkbox"/> Delete	<input type="checkbox"/> Read permissions
<input checked="" type="checkbox"/> Modify permissions	<input checked="" type="checkbox"/> Modify owner

OK Cancel

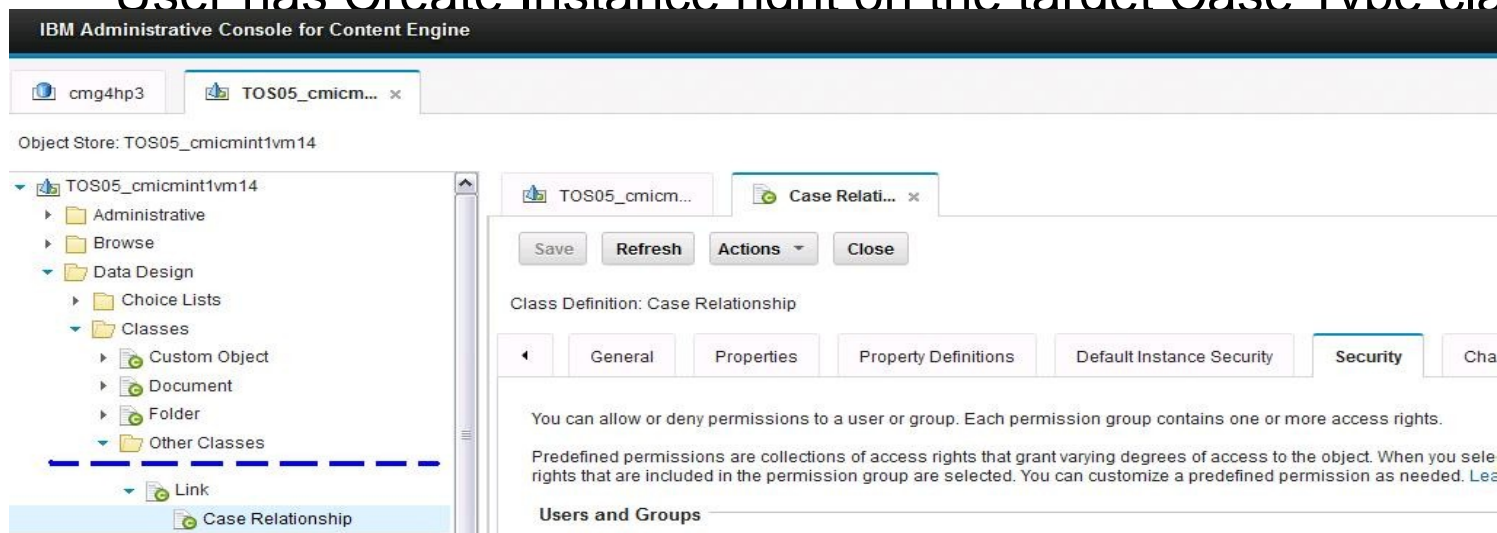
## Deployed Case Type Folder (cont.)

- Case Client UI actions will be grayed out unless user have proper rights
  - Some places missed will be enhanced in the future
  - But still protected properly in CPE backend

The screenshot displays the IBM Case Manager web application. The top navigation bar includes the 'IBM Case Manager' title, a user profile 'pwtest370', and the IBM logo. The main interface is divided into a left sidebar with a folder icon and a central content area. The content area has tabs for 'Cases' and 'Work', with the 'Cases' tab selected. Below the tabs, the case identifier 'Case SSD\_case1\_000000110001' is shown, along with the user 'Steven Security Demo | Auditor'. The case details section shows the case name 'SSD\_case1\_000000110001', its modification date '8/3/2013, 8:42 PM', and the case type 'case1'. Below this, there are buttons for 'Comments', 'Add Task', 'Add Custom Task', and 'Split Case', along with 'Save' and 'Close' buttons. The 'Documents' tab is active, showing a list of documents. The first document is 'sub1' with a modification date of '8/3/2013, 8:42 PM' by user 'pwtest350'. The second document is 'sub2' with the same modification date and user. To the right of the document list, there are input fields for 'b1', 'dt1' (with a date picker set to '8/4/2013' and a time picker set to '12:00 PM'), 'f1' (with value '200'), 'i1' (with value '200'), and 's1' (with value 'test 200').

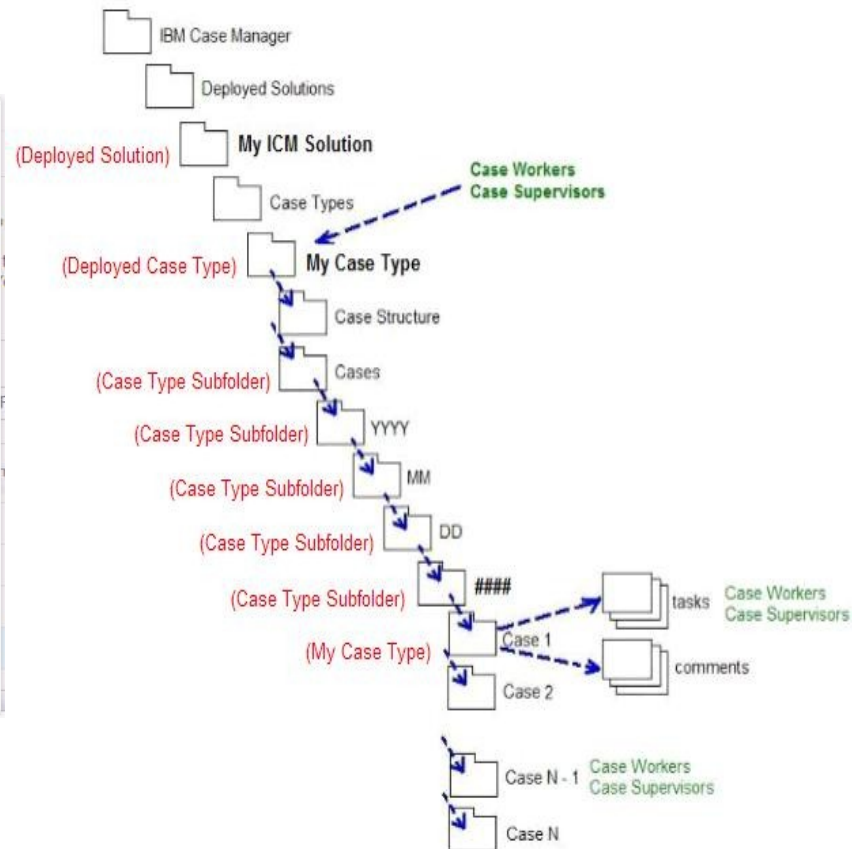
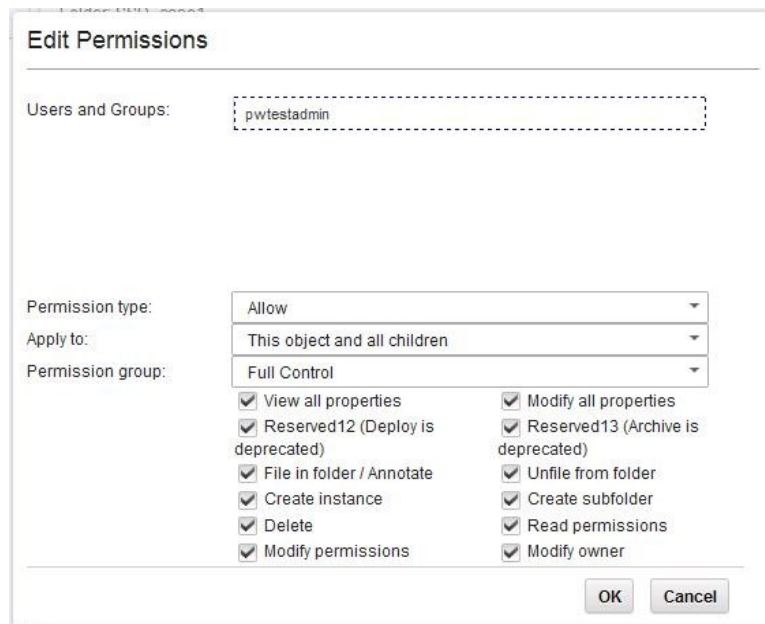
# Relate Cases and Split Case

- Cases can be related if the user can
  - View the cases to be related together
  - User has Create Instance right on the Case Relationship class
- A case can be split to another case of same or different case type
  - User has Create Instance right on the Case Relationship class
  - User has Create Instance right on the target Case Type class



# IT/ICM Solution Administrators

- Give IT/ICM Solution Administrators Full Control from Deployed Solution folder

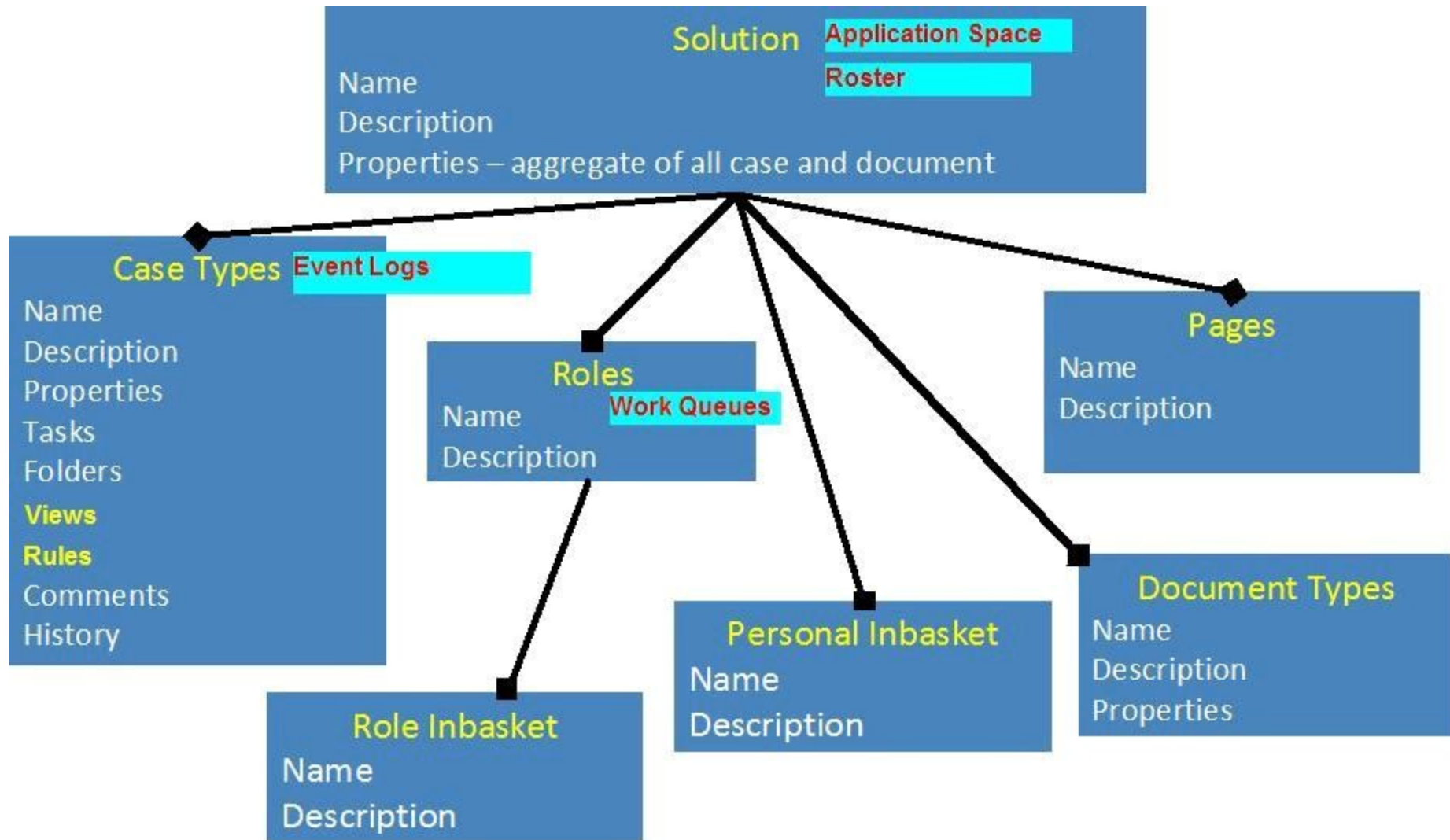




# Session Roadmap

- Target Environment Security Planning and Configuration
- ICM Solution Model and Solution Structure
- Case Manager Security Model
- Deployed Solutions and Case Client
- Content Engine Classes and Objects
- Process Services Queues, Event Logs, Roster and Application Space
- Additional Security Best Practices
- Q & A

# ICM Solution Model to Process Services



# Process Services

- A Process Region is shared by multiple ICM solutions
- Component Queues within a Process Region are shared by multiple ICM solutions
  - Already covered in previous section and security configured via Configuration Tool and Process Configuration Console
- Each ICM Solution → Application Space
  - Adjust Application Space security accordingly
  - Roles
    - Each Role has associated inbaskets and members
      - Setup role membership accordingly
- Each ICM Solution → Roster
  - Give Query and Create rights to case workers/managers who might need to start task processes
- Each Case Type → Event Log
- Each ICM Role → Work Queue
  - Inbasket definitions
  - Give members of the role Query and Process rights accordingly

# Process Services Security Model

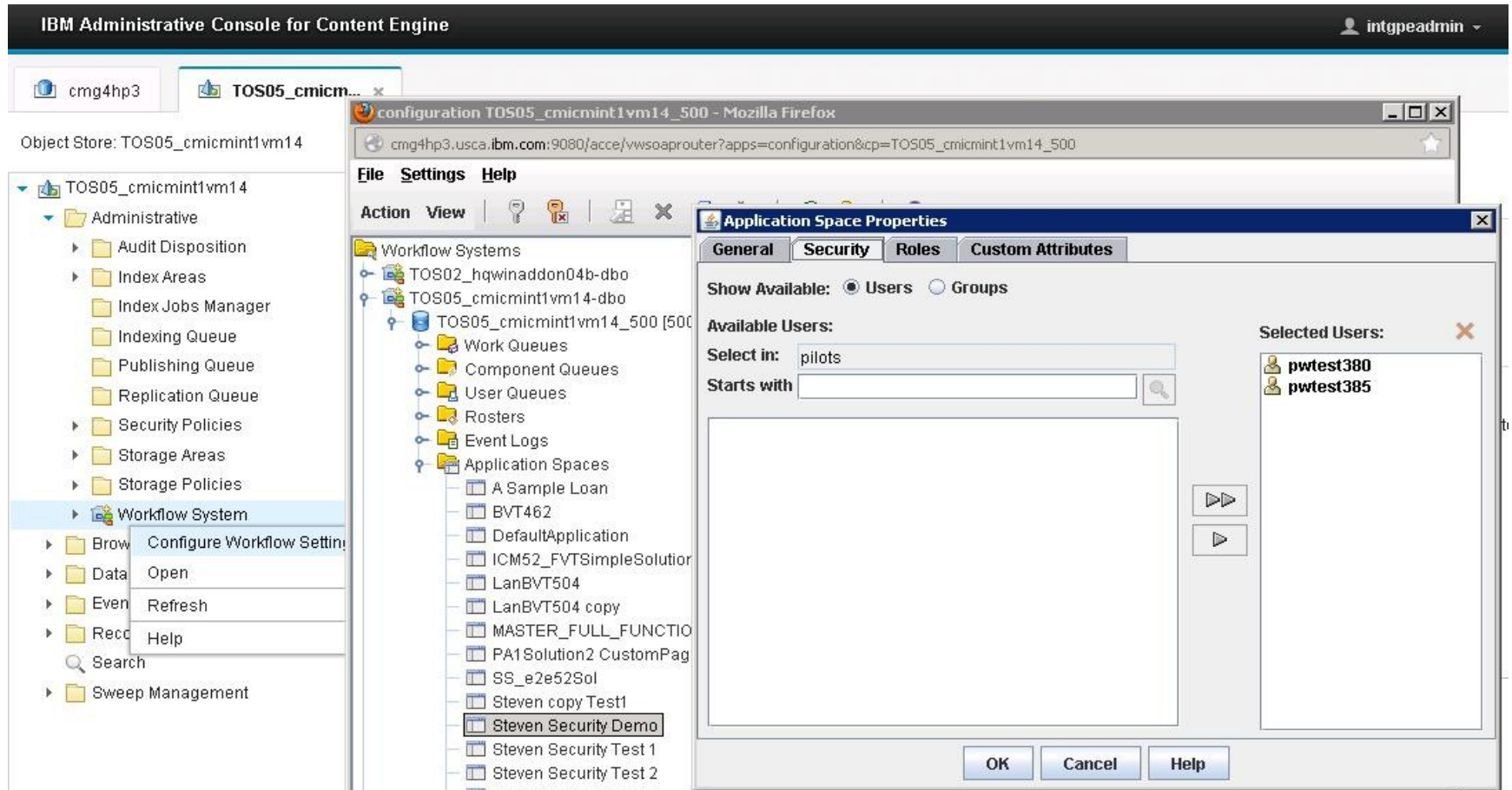
- Do not leave Process Services security open
  - A user can see and use 1 ICM solution does not mean that same user can see and use another solution deployed into same target environment
  - Only secured on CE side for each ICM Solution, each Case Type class, and case instances and assets are not sufficient, as Process Region is shared across ICM solutions as well
  - Process Services work item is as important as CE cases and assets
  - Work item may also contain important business information or sensitive private information during runtime even though not persisted into the case
  - PEREST and ICM/ICN model javascript APIs are exposed to client browser side to explore the system
  - Dynamic Task (Custom Task) if enabled for a Case Type, empowers certain workers to define and create ad-hoc processes directly off ICM Case Client
    - Not pre-determined by Business Analysis and tested like the system tasks and discretionary tasks
- Security practices should be planned, reviewed and applied accordingly by IT/ICM Solution Administrators as well

# Process Services Security Model (cont.)

- Setup Process Services Administrator and Configuration groups to IT/ICM Solution Administrators
  - Adjust remaining security based on solution security design
- Application Space (for the solution)
  - Users that can manage roles need to be added into Application Space security
  - No longer needs to be adjusted for Reassign Work to see all roles
- Roster (for the solution)
  - Controls task process creation/launching
  - Users who might start a task, e.g. during case creation, create and start a discretionary or custom task, etc. will need Create right
- Event Log (for each case type) – used by Case History/Visualizer
- Work Queue (for each role)
  - Query and Process rights to get to work object and process/dispatch
  - CE side security further influenced by the task processes design as well
  - User who can view/query the work items, select a response and influence how the work is routed next ... but can only view case
    - i.e. does not update case property, nor add document, etc.
  - User who can actually update the work item (case properties exposed on the step UI as R/W) with new values, add document, create comment, etc.

# Application Space

- Groups and users that can Manage Roles for a solution
  - No longer needs to be adjusted for Reassign Work to see all roles



# Roles

- Assign proper role membership for each role

The screenshot displays the IBM Administrative Console for Content Engine interface. The top navigation bar shows the user 'intgpeadmin'. The left sidebar shows the 'Object Store: TOS05\_cmicmint1vm14' with a tree view of folders including 'Administrative', 'Workflow System', and 'Workflow Systems'. The 'Workflow Systems' folder is expanded, showing a list of systems including 'TOS05\_cmicmint1vm14\_500 [500]'. The 'Application Space Properties' dialog box is open, showing the 'Roles' tab. The 'Partner' role is selected in the list on the left. The 'Description' field contains 'outside worker'. The 'URL for end-user home page' field is empty. The 'Select in-baskets and Members' section shows 'Partner' and 'SSD\_My Work' in the 'Select in-baskets f...' list, and 'pwtest350' and 'pwtest351' in the 'Select Members of this role' list. The 'OK', 'Cancel', and 'Help' buttons are at the bottom.



# Roster

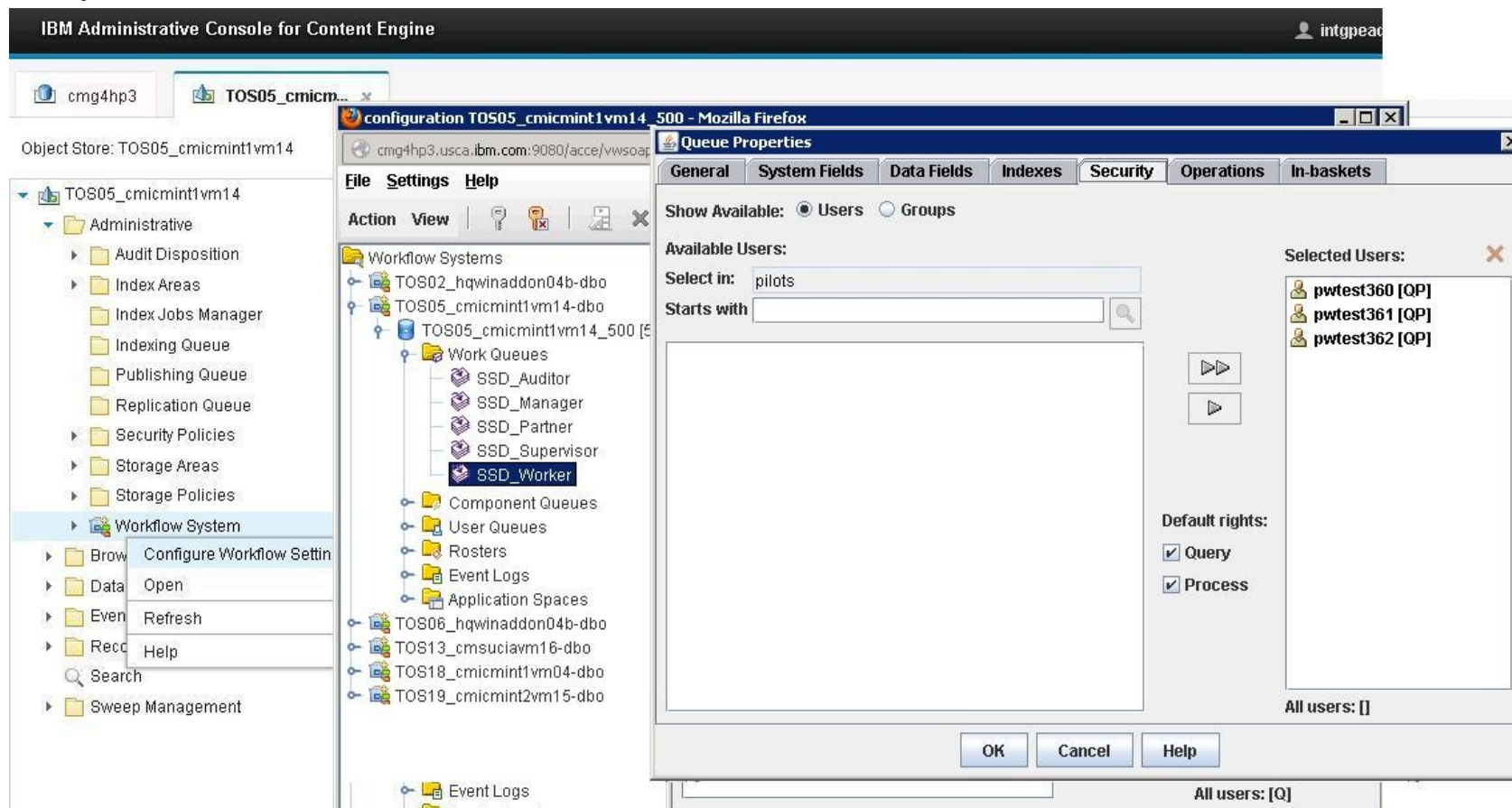
- Groups and users that can start task processes for a solution

The screenshot displays the IBM Administrative Console for Content Engine interface. The main window shows a tree view of the system structure, with the 'Workflow System' folder expanded. A context menu is visible over the 'Workflow System' folder, showing options like 'Configure Workflow Setting', 'Open', 'Refresh', and 'Help'. The 'Roster Properties' dialog box is open, showing the 'Security' tab. The 'Show Available' section has 'Users' selected. The 'Available Users' list includes 'pilots'. The 'Selected Users' list includes 'pwtest350 [C]', 'pwtest351 [C]', 'pwtest360 [C]', 'pwtest361 [C]', 'pwtest362 [C]', 'pwtest380 [C]', and 'pwtest385 [C]'. The 'Default rights' section has 'Query' and 'Create' checked. The 'All users: [Q]' button is at the bottom right.



# Work Queue

- Groups and users that can query and process work items for each work queue



# InBox Queue

IBM Administrative Console for Content Engine intgpeat

cmg4hp3 TOS05\_cmicm...

Object Store: TOS05\_cmicmint1vm14

TOS05\_cmicmint1vm14

- Administrative
  - Audit Disposition
  - Index Areas
  - Index Jobs Manager
  - Indexing Queue
  - Publishing Queue
  - Replication Queue
  - Security Policies
  - Storage Areas
  - Storage Policies
  - Workflow System
    - Configure Workflow Setting
    - Open
    - Refresh
    - Help
    - Search

Workflow Systems

- TOS02\_hqwinaddon04b-dbo
- TOS05\_cmicmint1vm14-dbo
  - TOS05\_cmicmint1vm14\_500 [500]
    - Work Queues
    - Component Queues
    - User Queues
      - Inbox
      - Tracker
    - Rosters
    - Event Logs
    - Application Spaces
  - TOS06\_hqwinaddon04b-dbo
  - TOS13\_cmsuciavm16-dbo

Queue Properties

General System Fields Data Fields Indexes Security Operations In-baskets

Show Available: ☒ Users ☐ Groups

Available Users:

Select in: pilots

Starts with

Selected Users:

Default rights:

☒ Query

Queue Properties

General System Fields Data Fields Indexes Security Operations In-baskets

In-baskets

SSD\_My Work

SSD\_All Assigned Work

SSD\_All Assigned Work

Create Columns and Labels Create filters Define Content Custom Attributes


Define in-basket columns for the user interface

Selected fields	Column label	Sortable	Content order
F_StepName (String)	Step Name	<input type="checkbox"/>	<none>
F_CreateTime (Time)	Time Created	<input type="checkbox"/>	<none>
F_Subject (String)	Subject	<input type="checkbox"/>	<none>

# Show In-basket for All Assigned Work

IBM Case Manager Builder Intgpeadmin ?

Manage Solutions \ **Steven Security Test 3** Show Locked Items Validate Save Save and Close Close

**Steven Security Test 3**  
Steven Security Test 3   
Solution prefix: SST3  
Created by pwtest370  
Created on July 20, 2013

Properties **Roles** In-baskets Document Types Pages Case Types

Add Role OK All

**Partner** outside worker

**Worker** back office worker

\* Role:  Description:  OK Cancel

**Role Settings** **Pages**

In-baskets currently associated with this role: Supervisor, All Assigned Work, My Work

Select the type of personal in-basket to display for this role:

☒ Personal (Common): Show the common view

☐ Personal (Role): Show a custom view for this role

☐ Do not show common or role personal in-baskets

Work assignment options to display for this role:

☒ Role members can move work into their personal in-basket

☒ Role members can reassign work to others

Assignment in-basket

☒ Show the in-basket that displays all assigned work

**Manager**

# In-basket for All Assigned Work for a Role

The screenshot displays the IBM Administrative Console for Content Engine. The top navigation bar includes the IBM logo, the user 'intgpeadmin', and various system icons. The main interface is divided into several panes:

- Left Pane:** A tree view showing the hierarchy of the system. The 'Workflow System' is selected under 'TOS05\_cmimint1vm14'.
- Center Pane:** A tree view of the 'Workflow Systems' under 'TOS05\_cmimint1vm14\_500'. The 'Application Spaces' folder is expanded, showing a list of application spaces including 'Steven Security Demo'.
- Right Pane:** The 'Application Space Properties' dialog box, with the 'Roles' tab selected. It shows a list of roles: Partner, Worker, Supervisor (highlighted), Manager, and Auditor. Below this, the 'Supervisor' role is configured with a description of 'back office supervisor'. The 'Select in-baskets and Members' section shows the role assigned to 'Supervisor' with in-baskets 'SSD\_All Assigned Work' and 'SSD\_My Work'. The 'Select Members of this role' section shows the member 'pwtest380'.

# Role with All Assigned Work

IBM Case Manager

pwtest380

IBM

Cases

Work

Steven Security Demo | Supervisor

Manage Roles

Add Case

Supervisor (0)

All Assigned Work (2)

My Work

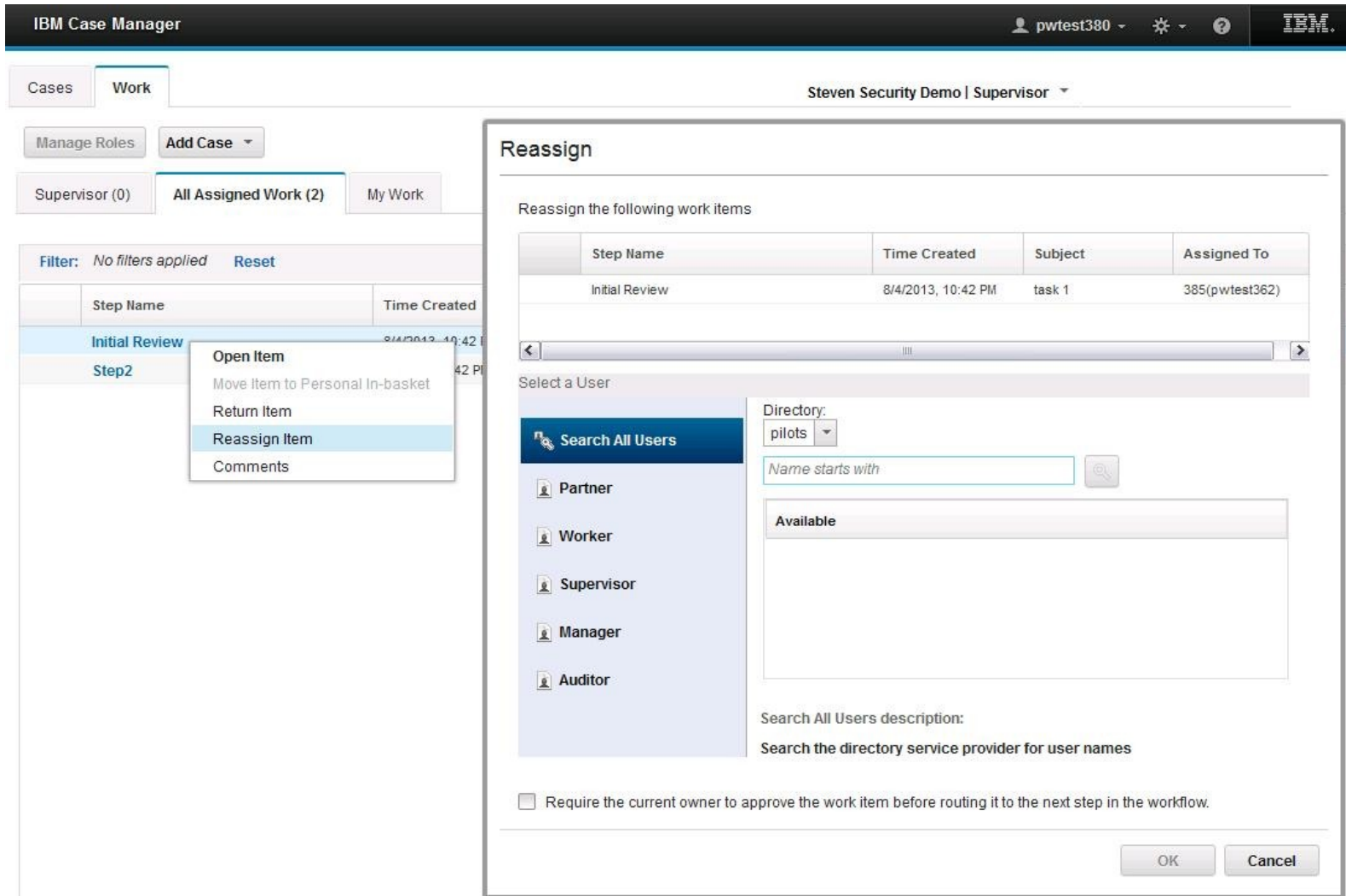
Filter: No filters applied

Reset

Step Name	Time Created	Subject	Assigned To	
Initial Review	8/4/2013, 10:42 PM	task 1	385(pwtest362)	
Step2	8/3/2013, 8:42 PM	case start	387(pwtest360)	



# Reassign Work



The screenshot shows the IBM Case Manager interface with a 'Reassign' dialog box open. The background interface includes a top navigation bar with 'IBM Case Manager', a user profile 'pwtest380', and an IBM logo. Below this is a 'Cases' and 'Work' tab bar, with 'Work' selected. A 'Steven Security Demo | Supervisor' dropdown is visible. On the left, there are buttons for 'Manage Roles' and 'Add Case', and a filter section showing 'Supervisor (0)', 'All Assigned Work (2)', and 'My Work'. A table lists work items with columns 'Step Name' and 'Time Created'. The 'Initial Review' item is selected, and a context menu is open with options: 'Open Item', 'Move Item to Personal In-basket', 'Return Item', 'Reassign Item' (highlighted), and 'Comments'.

**Reassign**

Reassign the following work items

Step Name	Time Created	Subject	Assigned To
Initial Review	8/4/2013, 10:42 PM	task 1	385(pwtest362)

Select a User

Search All Users

- Partner
- Worker
- Supervisor
- Manager
- Auditor

Directory: pilots

Name starts with

Available

Search All Users description:  
Search the directory service provider for user names

☐ Require the current owner to approve the work item before routing it to the next step in the workflow.

OK Cancel

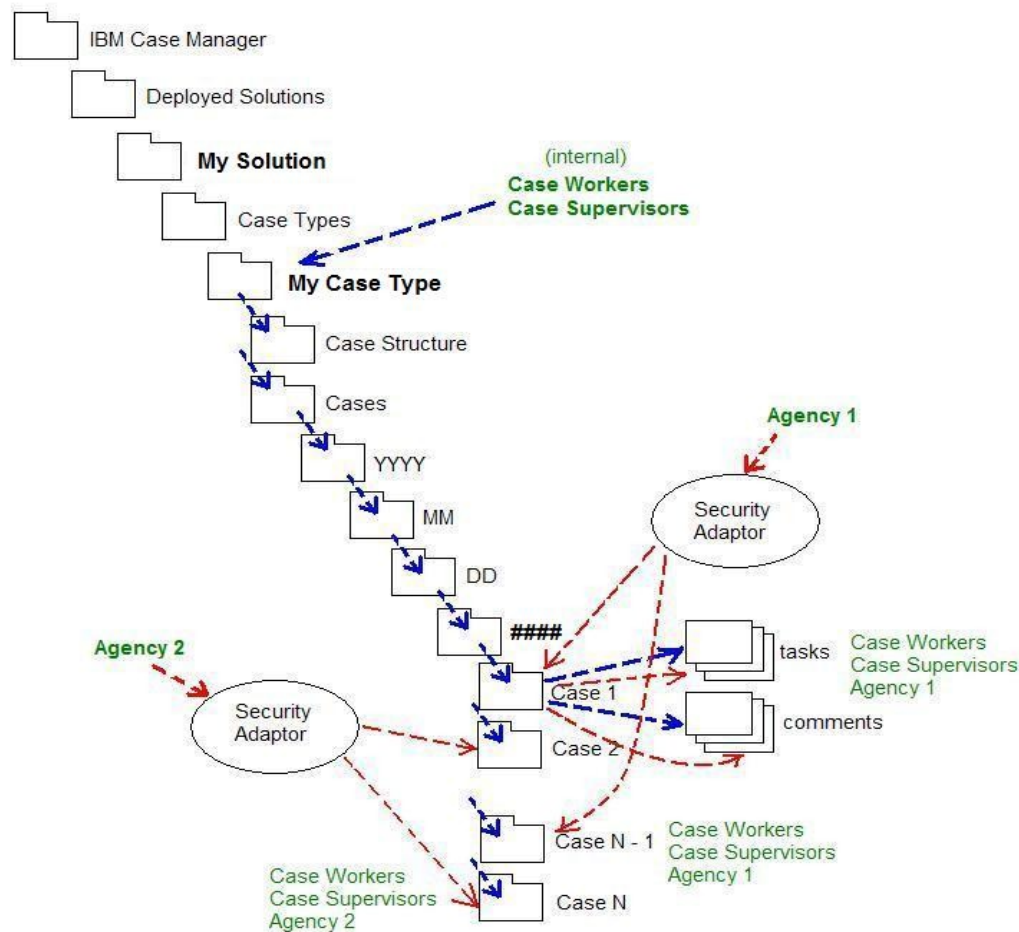


# Session Roadmap

- Target Environment Security Planning and Configuration
- ICM Solution Model and Solution Structure
- Case Manager Security Model
- Deployed Solutions and Case Client
- Content Engine Classes and Objects
- Process Services Queues, Event Logs, Roster and Application Space
- ➔Additional Security Best Practice
- Q & A

## Security Adaptor/Proxy Mix-in

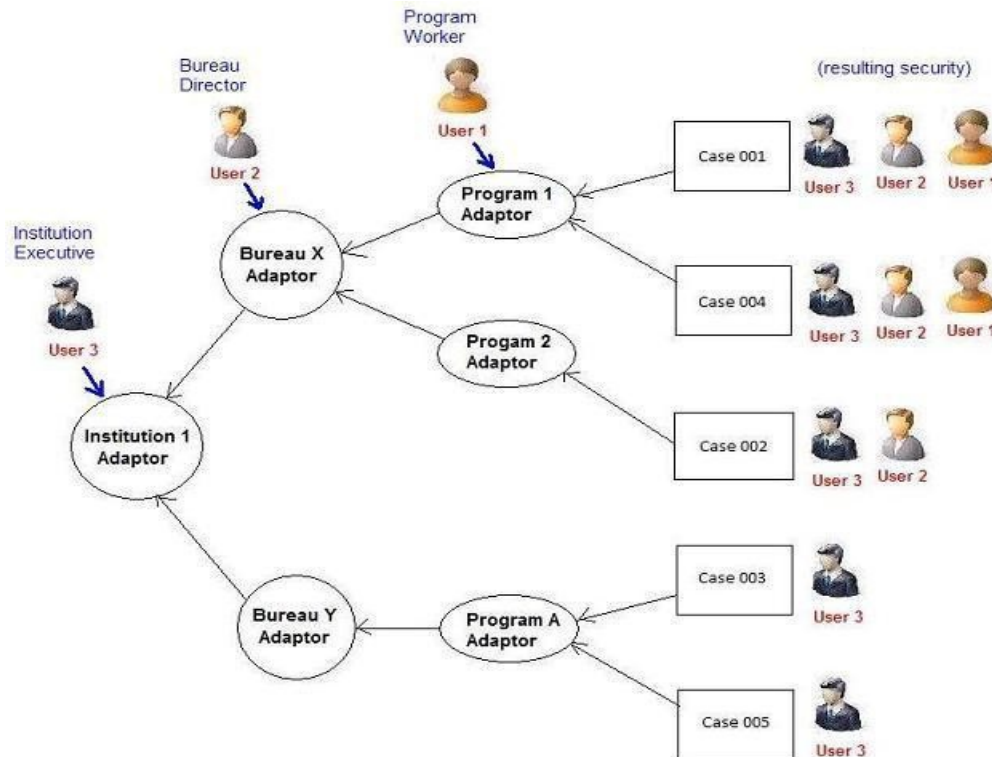
- A subset of the cases now have different security rights mixed in
- Still a limited set of control points to adjust security as needed





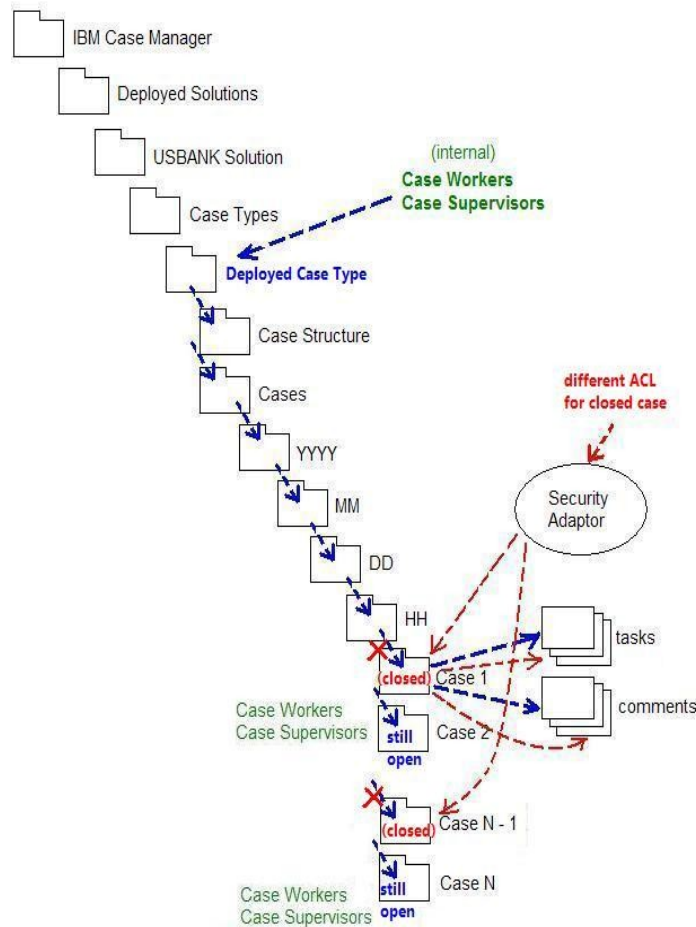
# Security Adaptor/Proxy Hierarchy

- Build a security adaptor hierarchy according to organizational structure or security privilege hierarchy
- Simple adjustment of security proxy pointers (OVPs) to reflect the security changes needed
  - e.g. Program 2 now under supervision of Bureau Y



## Security Adaptor change based on Case State

- A subset of the cases at different states/stages now can have different security rights mixed in or completely replaced
  - An alternative of using marking set to achieve this

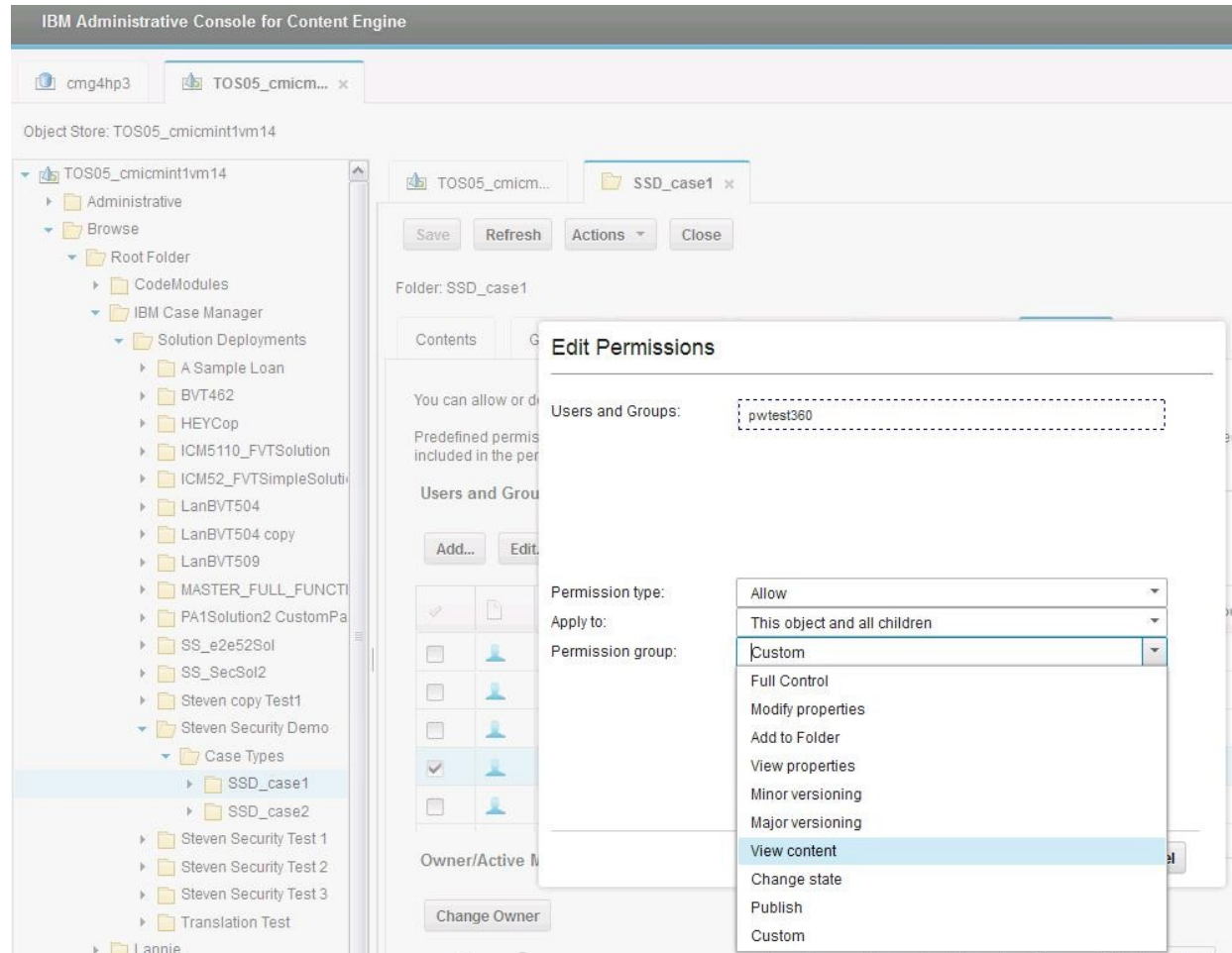


# Case Owned Documents

- In a lot of case management scenarios, case documents added to a case are owned by the case
  - They are there to support that particular case solely, and not shared/filed to any other case
  - There could be a lot of different document classes involved in a case
- A common scenario is
  - Anyone who gets added to handle a case dynamically, the worker can and should be able to view or even update any document filed in the case as well
- However
  - All possible document classes involved can not be predicted, and default instance security can not be pre-determined
  - Adjust all document instances' security already in the case is not a good approach and sometimes not even feasible whenever a group/user is removed or assigned to handle the case

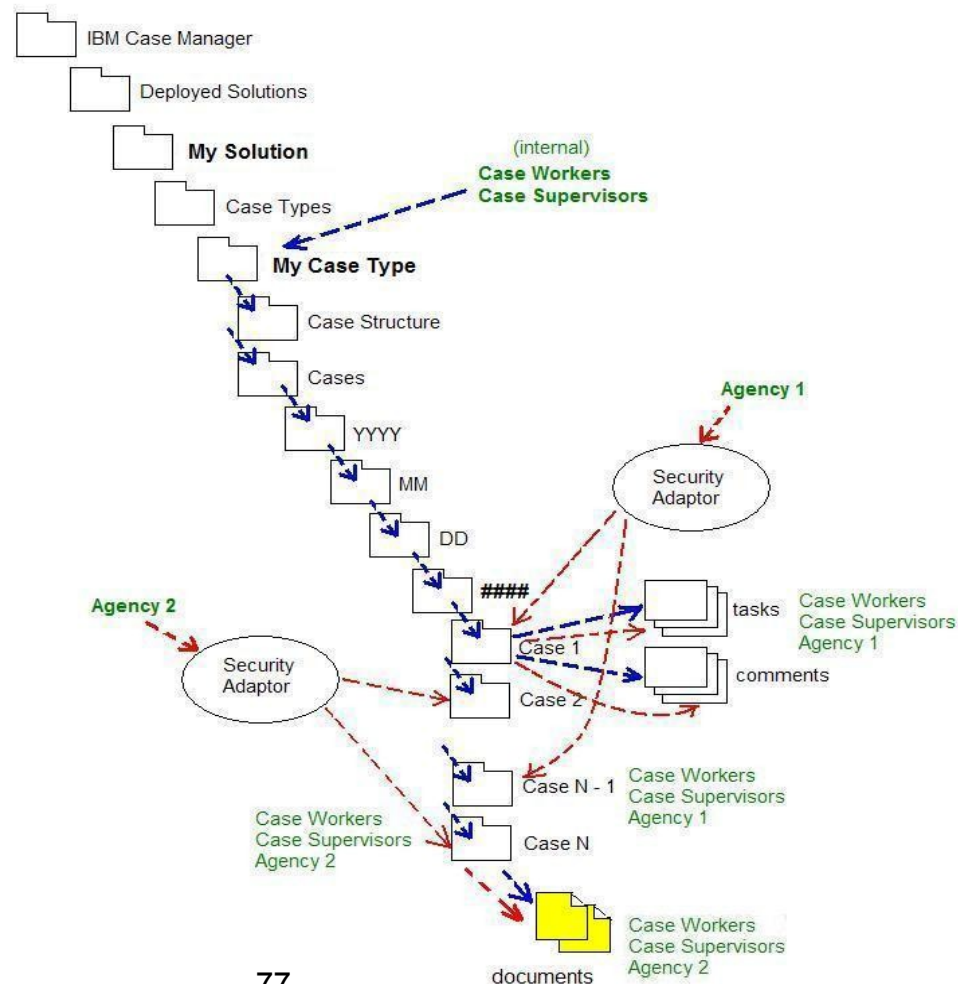
# Case Owned Documents (cont.)

- Configure the deployed case type folder or security adaptor to also propagate View Content or even Major Versioning



# Case Owned Documents (cont.)

- Setup security folder of the document to the case folder or case subfolder
  - Allows security to be propagated from container to the document



# Session Roadmap

- Target Environment Security Planning and Configuration
- ICM Solution Model and Solution Structure
- Case Manager Security Model
- Deployed Solutions and Case Client
- Content Engine Classes and Objects
- Process Services Queues, Event Logs, Roster and Application Space
- Additional Security Best Practices

→ Q & A

# Questions

