Course Guide

Configure IBM Case Manager Security (V5.3.2)

Course code F2920G ERC 1.0

IBM Training

June 2018

NOTICES

This information was developed for products and services offered in the USA.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service. IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

TRADEMARKS

IBM, the IBM logo, ibm.com, FileNet, and WebSphere are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Adobe, and the Adobe logo, are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Contents

Course overview

Preface overview

In this course you will configure security for IBM Case Manager environments and solutions. You will work with project areas, control access to cases, and create security configurations. You will deploy a solution in a new environment and use a security configuration package file to manage solution security. You will customize security settings with a custom privilege definition and use security proxies to automate security changes.

Intended audience

This course is for system administrators who maintain IBM Case Manager environments and for solution architects who must plan security requirements for their solutions.

Topics covered

Topics covered in this course include:

- Overview of security deployment
- Work with project areas
- Manage access to cases
- Create a security configuration
- Configure target object store security
- Configure deployed solution security
- Customize a privilege definition
- Use security proxies
- Automate case security changes
- Additional security configurations

Course prerequisites

Participants should have:

- Knowledge of Case Manager concepts, such as case management, case, solution, task.
- Ability to build, validate, deploy, and test solutions.
- Completed the Build an IBM Case Manager Solution V5.3.2 (classroom - F2910G or self-paced - F2919G)

Document conventions

Conventions used in this guide follow Microsoft Windows application standards, where applicable. As well, the following conventions are observed:

- **Bold**: Bold style is used in demonstration and exercise step-by-step solutions to indicate a user interface element that is actively selected or text that must be typed by the participant.
- **`Bold style + Courier New font`** is used for text that must be typed by the participant.
- *Italic*: Used to reference book titles.
- CAPITALIZATION: All file names, table names, column names, and folder names appear in this guide exactly as they appear in the application.
  To keep capitalization consistent with this guide, type text exactly as shown.

Exercises

Exercise format

Exercises are designed to allow you to work according to your own pace. Content contained in an exercise is not fully scripted out to provide an additional challenge. Refer back to demonstrations if you need assistance with a particular task. The exercises are structured as follows:

The business question section

This section presents a business-type question followed by a series of tasks. These tasks provide additional information to help guide you through the exercise. Within each task, there may be numbered questions relating to the task. Complete the tasks by using the skills you learned in the unit. If you need more assistance, you can refer to the Task and Results section for more detailed instruction.

The task and results section

This section provides a task based set of instructions that presents the question as a series of numbered tasks to be accomplished. The information in the tasks expands on the business case, providing more details on how to accomplish a task. Screen captures are also provided at the end of some tasks and at the end of the exercise to show the expected results.

Additional training resources

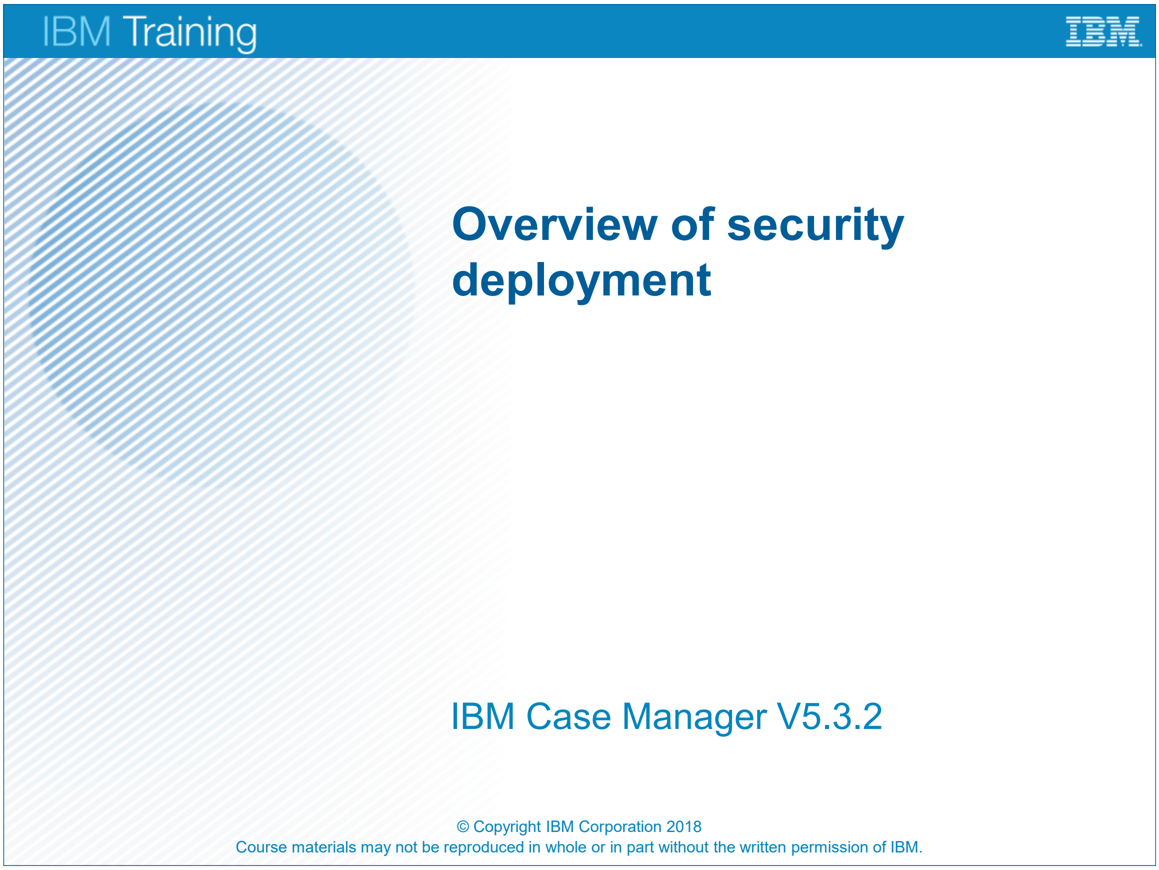
Visit the IBM Skills Gateway (www.ibm.com/training/) for details on:

- Instructor-led training in a classroom or online
- Self-paced training that fits your needs and schedule
- Comprehensive curricula, learning journeys, and training paths that help you identify the courses that are right for you
- IBM Professional Certification Program (http://www-03.ibm.com/certify/)
- For other resources that will enhance your success, bookmark the IBM Analytics Skills Gateway (https://www-03.ibm.com/services/learning/ites.wss/zz-en?pageType=page&c=C067650S63836C42)

IBM product help

Help type	When to use	Location
Task-oriented	You are working in the product and you need specific task-oriented help.	IBM Knowledge Center https://www.ibm.com/support/knowledgecenter/SSCTJ4_5.3.2/com.ibm.casemgmttoc.doc/casemanager_5.3.2.htm
Books for Printing (.pdf)	You want to use search engines to find information. You can then print out selected pages, a section, or the whole book. Use Step-by-Step online books (.pdf) if you want to know how to complete a task but prefer to read about it in a book. The Step-by-Step online books contain the same information as the online help, but the method of presentation is different.	Start/Programs/*IBM Product*/Documentation
IBM on the Web	You want to access any of the following:	
	• IBM Skills Gateway	• https://www-03.ibm.com/services/learning/ites.wss/zz-en?pageType=page&c=a0011023
	• Online support	• https://www.ibm.com/support/home/
	• IBM Web site	• http://www.ibm.com

Unit 1 Overview of security deployment

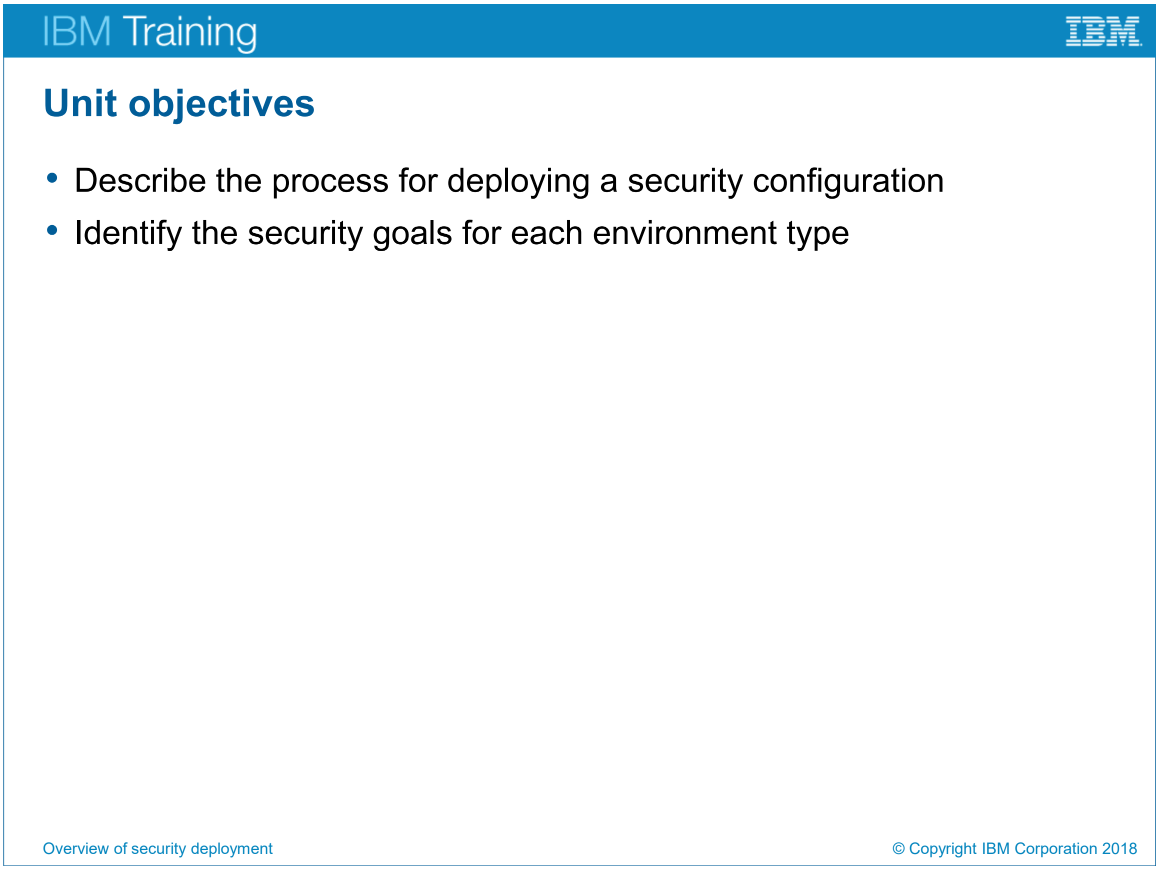


IBM Training

IBM

Overview of security deployment

IBM Case Manager V5.3.2



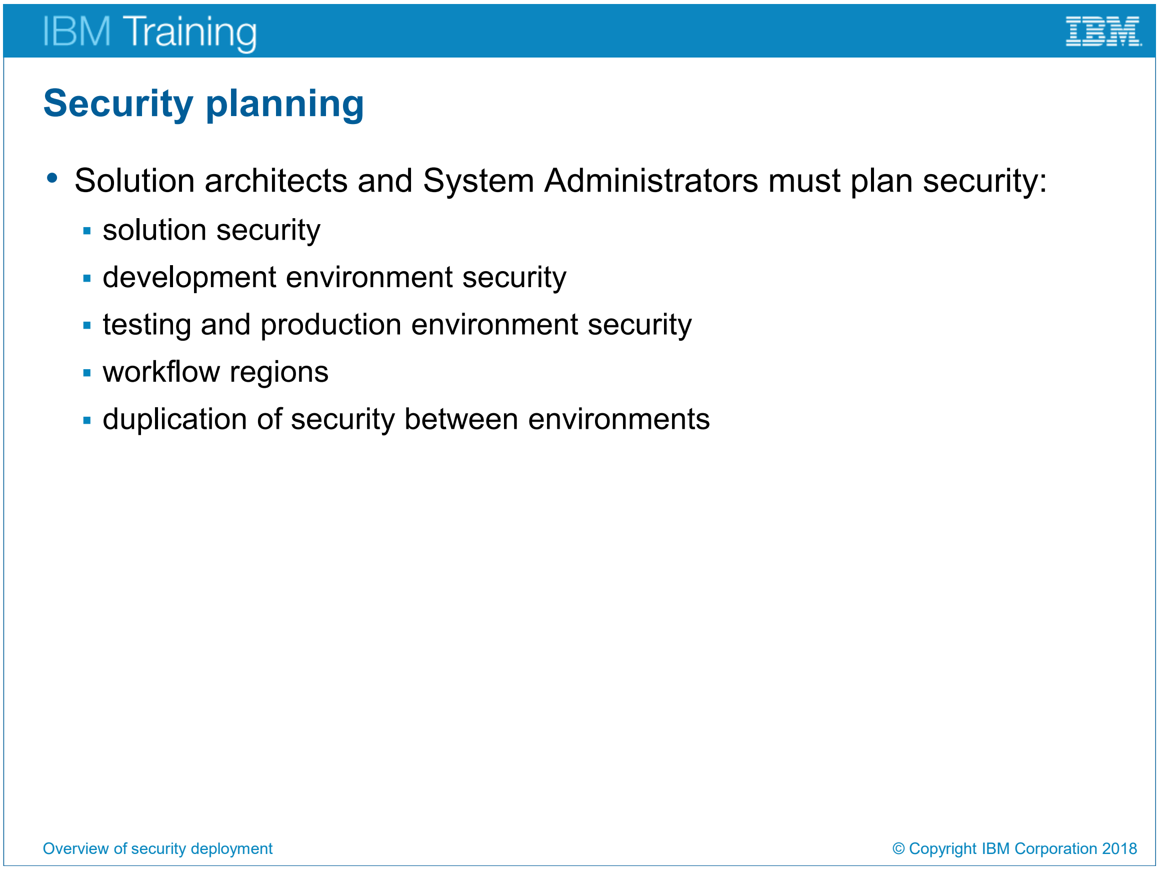
IBM Training

Unit objectives

- Describe the process for deploying a security configuration
- Identify the security goals for each environment type

Overview of security deployment

Unit objectives



IBM Training

Security planning

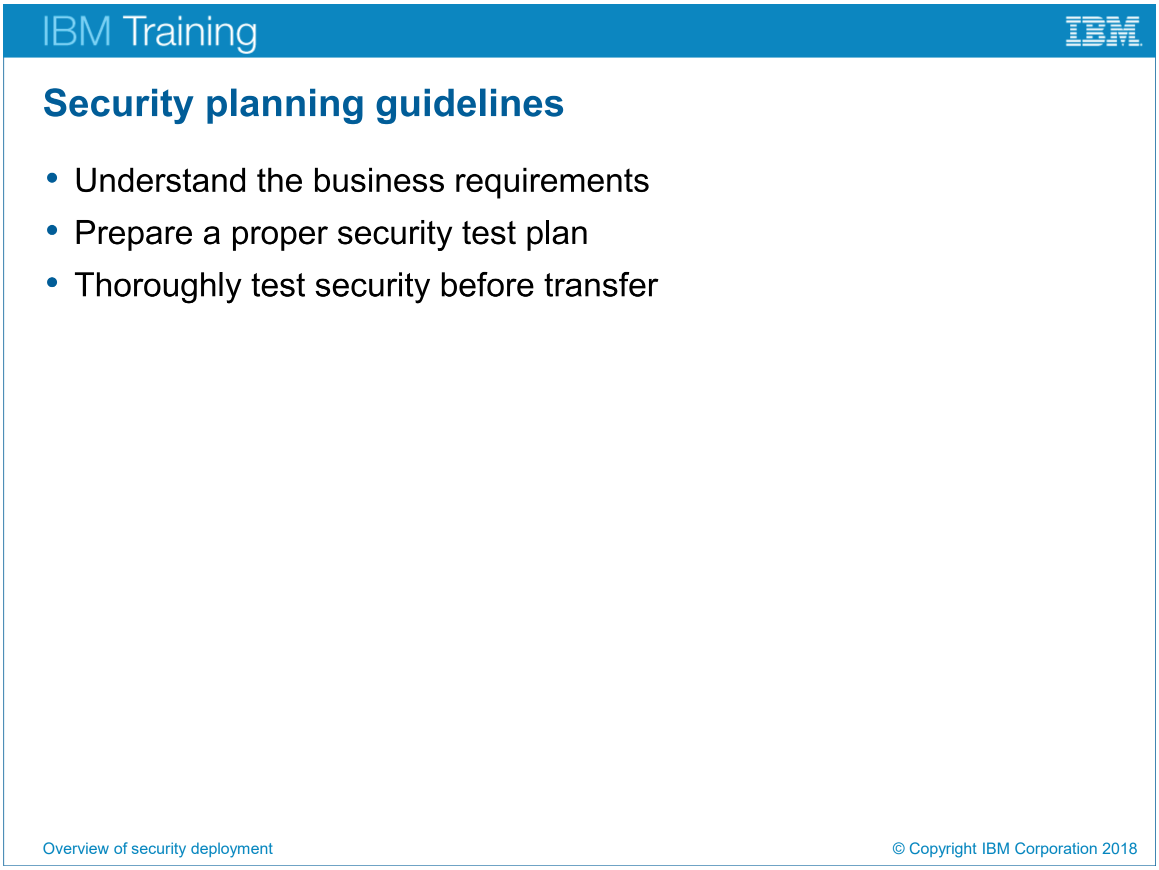
- Solution architects and System Administrators must plan security:
  - solution security
  - development environment security
  - testing and production environment security
  - workflow regions
  - duplication of security between environments

Overview of security deployment

Security planning

Before you begin to build the solution, you must plan your approach to securing the solution. Solution architects and system administrators must carefully plan security for the following areas:

- The Solution architect must plan security for solutions, including roles, pages, solution objects, and workflows.
- The system administrator must manage development environment security, testing and production environment security, workflow regions, and the duplication of security between environments.



IBM Training

Security planning guidelines

- Understand the business requirements
- Prepare a proper security test plan
- Thoroughly test security before transfer

Overview of security deployment

© Copyright IBM Corporation 2018

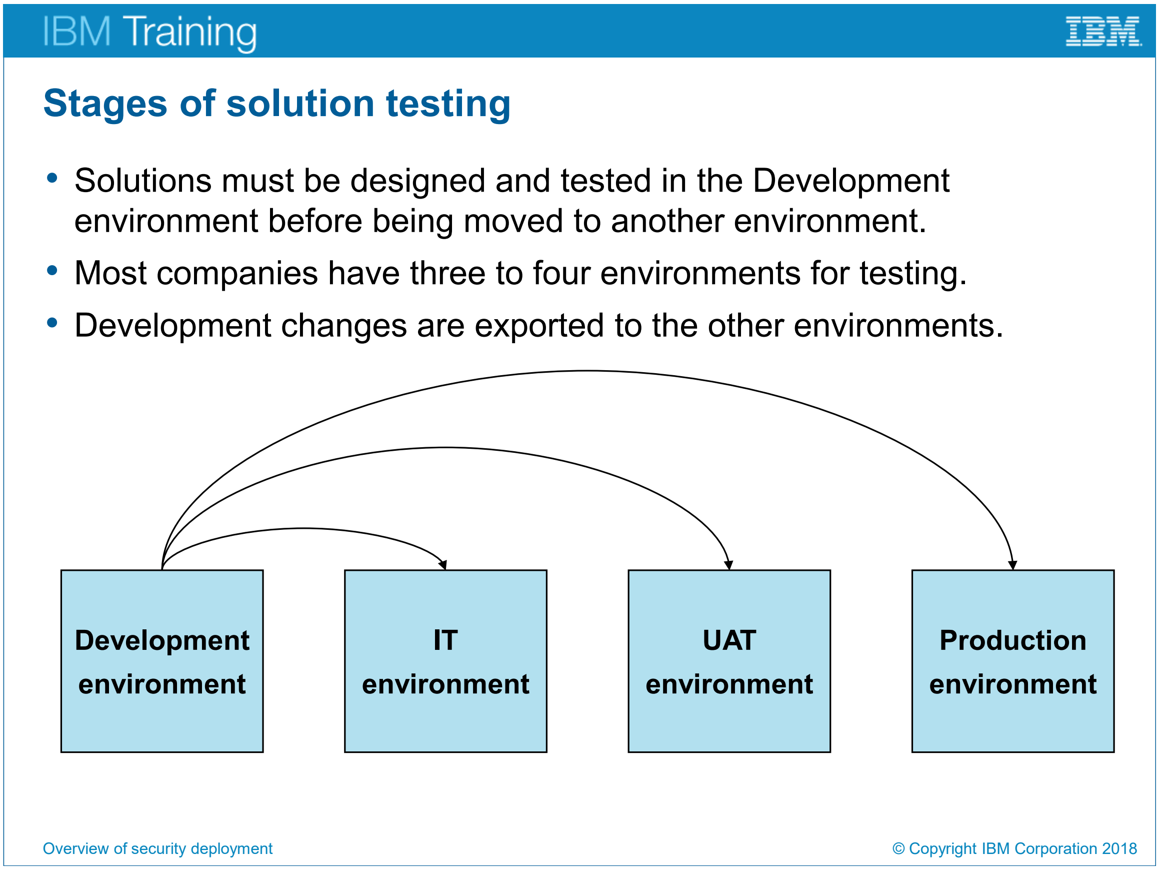
Security planning guidelines

Security is one of the most important aspects of a solution and it is important to get it right before you deploy the solution into production. Plan security throughout the development process. For example, you must consider object store security before you create the object store.

Understand the business requirements of the customer as well as security models needed before you build the solution. Design the solution accordingly.

Prepare a proper security test plan. Include scenarios and allocate sufficient time to exercise the plan.

Understand and thoroughly test security before you migrate and deploy the solution to user acceptance testing (UAT), production, or to a client site.



IBM Training

Stages of solution testing

- Solutions must be designed and tested in the Development environment before being moved to another environment.
- Most companies have three to four environments for testing.
- Development changes are exported to the other environments.

Development environment

IT environment

UAT environment

Production environment

Overview of security deployment

© Copyright IBM Corporation 2018

Stages of solution testing

A solution development lifecycle requires that the solution moves to different environments. You must configure security for each environment according to the requirements of both the environment and the solution.

Every organization might have different solution testing stages. A representative example includes a development stage, integration testing, user acceptance testing, and then production.

Solutions are designed and tested in the Development environment. After they are fully tested, they are transferred to another environment for more thorough testing. Most companies have three to four stages of testing environments.

You test security throughout the solution development and testing lifecycle. All changes to the solution are made in the Development environment. For each testing stage, the solution is deployed to a testing environment. During the process of migrating to new environments, the solution migration and deployment process is carefully documented so that it is replicable.

For training purposes, only two environments are used in this course: a Development environment and a UAT environment.

The Development environment is for testing basic solution design, such as workflow and document properties. This environment is the source control for the solution.

Design is iterative, in that the solution might undergo many versions of redesign and retesting in this environment. Security is open to allow testers easy access to the solution. Security testing is not possible in this environment.

The IT environment is where security testing usually begins. The environment is configured to have a security structure similar to the security structure that is used in production. Document the migration and deployment procedures so that it can be easily reproduced.

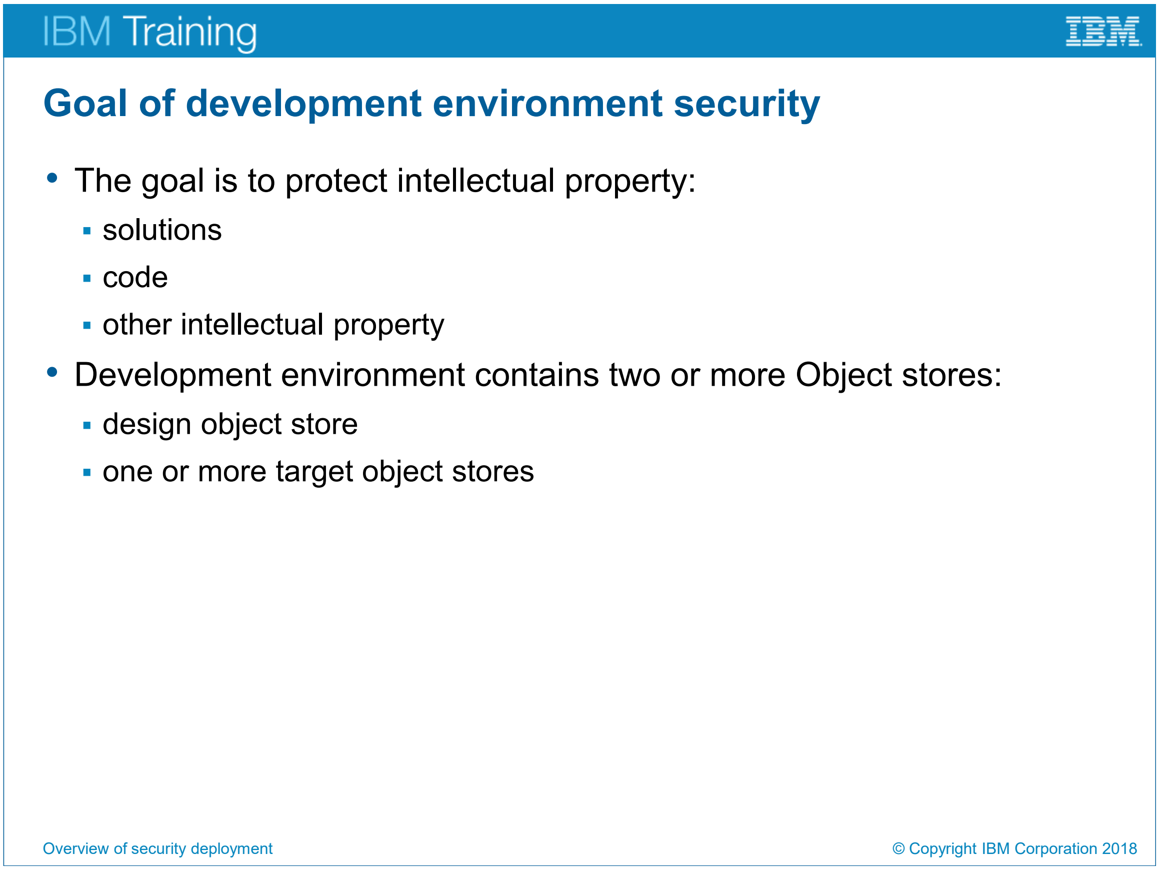
The User Acceptance Testing environment is designed to ensure that users accept how the solution works. Security details are worked out. Fix all security gaps before the solution is moved to Production.

The early stages use a development type environment. Later testing and staging use a non-development environment and have a production profile.

Use the source-control guidelines to ensure greater control of your solution package.

You can import and deploy the same solution package across the different environments.

Edit only the files in the Development environment to ensure that you have a consistent solution package with clear version control and history.



IBM Training

Goal of development environment security

- The goal is to protect intellectual property:
  - solutions
  - code
  - other intellectual property
- Development environment contains two or more Object stores:
  - design object store
  - one or more target object stores

Overview of security deployment

© Copyright IBM Corporation 2018

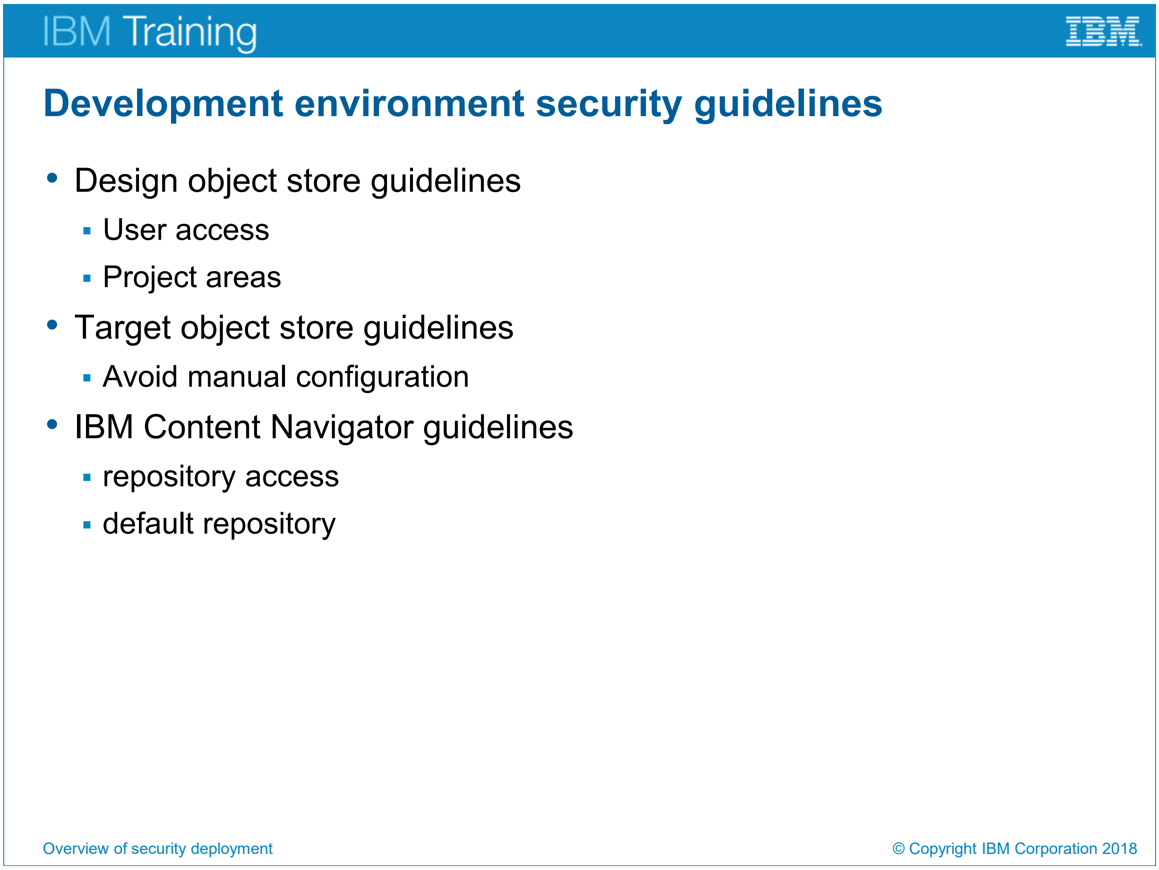
Goal of development environment security

The system administrator is responsible for managing security across environments. The system administrator typically configures security for the Development environment.

The goal of security for the Development environment is to protect the solution, code, and other intellectual property from unauthorized access.

The Development environment contains two or more object stores:

- A Design object store, which contains the solution and workflow definition files.
- One or more Target object stores, which contain the deployed solutions.



IBM Training

Development environment security guidelines

- Design object store guidelines
  - User access
  - Project areas
- Target object store guidelines
  - Avoid manual configuration
- IBM Content Navigator guidelines
  - repository access
  - default repository

Overview of security deployment

© Copyright IBM Corporation 2018

Development environment security guidelines

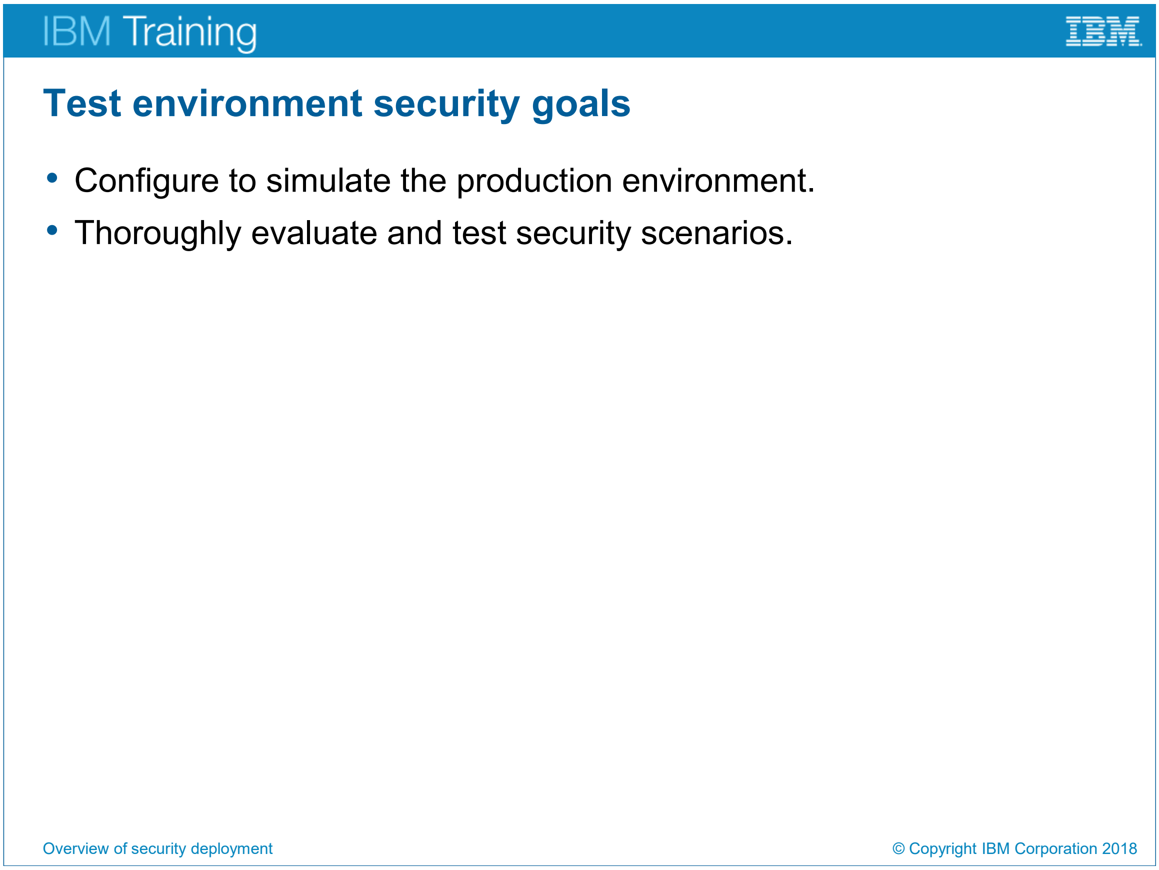
Use the following guidelines when you set up a design object store:

- A user must first have access to the Design and Target object stores before any solution building is possible.
- Adding a user to a project area gives the user access to the solutions in the project area in the design object store.

Because Case Manager Client uses the IBM Content Navigator structure, you need to know how to secure IBM Content Navigator.

IBM Content Navigator guidelines:

- Case Manager Client is based on an IBM Content Navigator desktop.
- Users who access Case Manager Client must have access to the default repository that is defined for the Case Manager desktop.
- In Development environments, the default repository is the Design object store.



IBM Training

Test environment security goals

- Configure to simulate the production environment.
- Thoroughly evaluate and test security scenarios.

Overview of security deployment

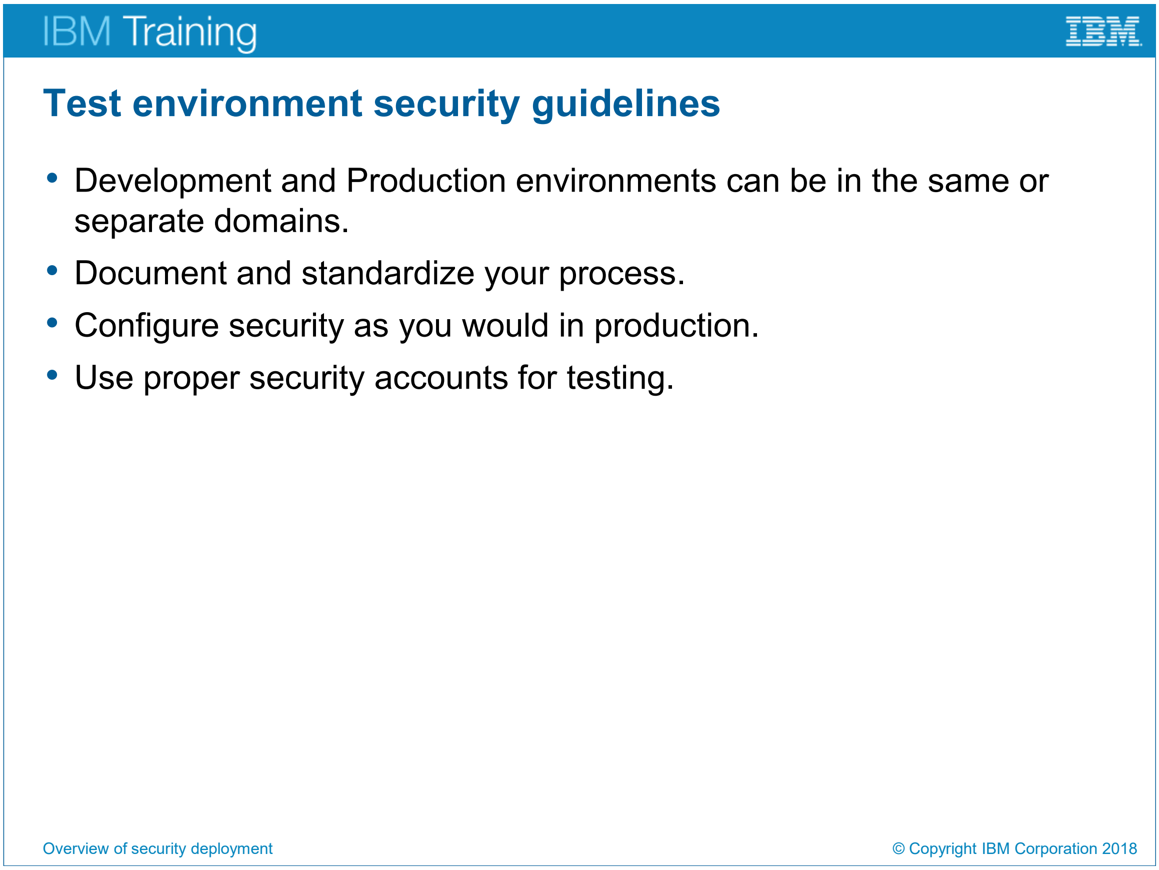
© Copyright IBM Corporation 2018

Test environment security goals

Security must not be overlooked during testing. Security in the testing environment must be configured as near as possible to security in the production environment.

The main goal of security in the Test environment is to simulate the security model of the Production environment. You can test security in this environment without exposing security problems in the production environment.

Ensure that all security-related issues are resolved before you move the solution to production.



IBM Training

Test environment security guidelines

- Development and Production environments can be in the same or separate domains.
- Document and standardize your process.
- Configure security as you would in production.
- Use proper security accounts for testing.

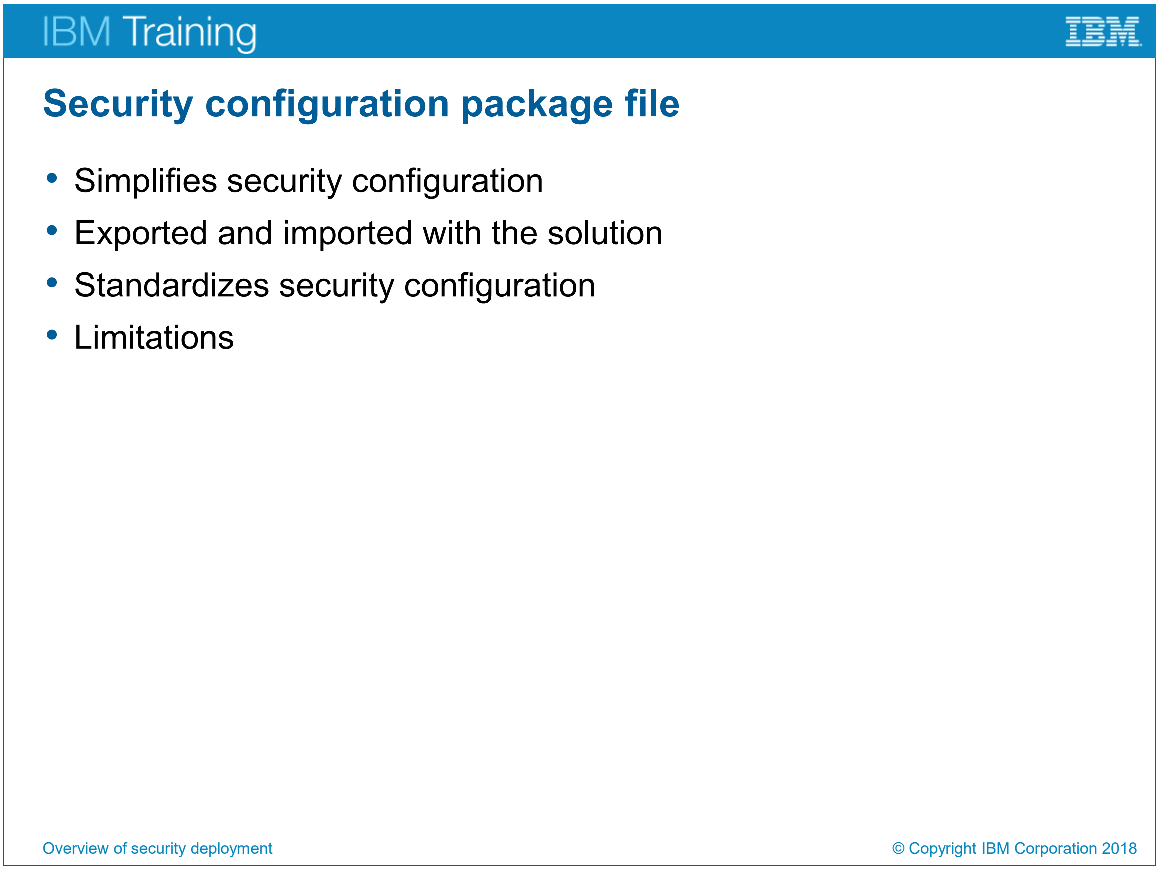
Overview of security deployment

© Copyright IBM Corporation 2018

Test environment security guidelines

Follow these guidelines when you set up a target environment for testing:

- The Development environment and Production environment (and IT/UAT) can be within the same Content Platform Engine domain or multiple domains.
- Document and standardize the process of migrating the solution from Development to UAT. If any security settings are manually configured, then you must document those.
- Configure security for a deployed solution the same as in a production environment.
- Use proper end-user accounts for security tests. For example, do not sign in as Administrator to Case Manager Client.



IBM Training

Security configuration package file

- Simplifies security configuration
- Exported and imported with the solution
- Standardizes security configuration
- Limitations

Overview of security deployment

© Copyright IBM Corporation 2018

Security configuration package file

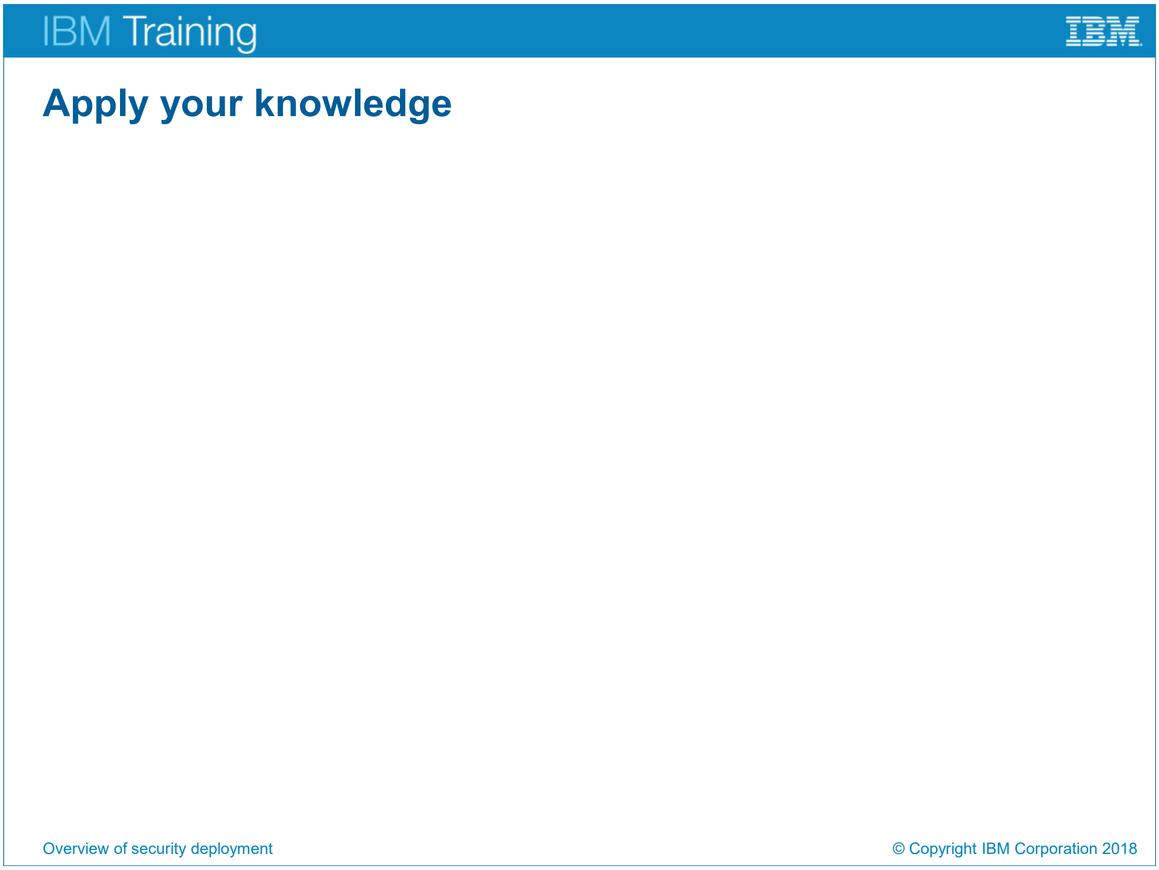
Part of the process of migrating and deploying solutions between environments is handling the security configuration package file. The security configuration package file is a file that defines roles and permissions that you can export and import with a solution. After you deploy the solution, you can use this file to apply the security settings.

The security configuration package file has some limitations. It does not properly handle the following types of artifacts:

- Artifacts that are transferred with FileNet Deployment Manager.
- Security adaptors or proxies.
- Default instance security.

If you rely on these types of artifacts, you must configure security using manual steps.

You must test the Security Configuration thoroughly in a testing environment before you apply it to the production environment.



IBM Training

Apply your knowledge

Overview of security deployment

Apply your knowledge

Apply your knowledge

In this unit, you learned about security goals for stages of solution development. Complete the short quiz to confirm that you understand the concepts.

Questions

1. What is the main goal of security on the Development environment?

   a. Prevent unauthorized access to personal information.

   b. Prevent unauthorized access to customer information.

   c. Prevent unauthorized access to object stores.

   d. Prevent unauthorized access to intellectual property.

2. What is the main goal of security on the UAT environment?

   a. Prevent unauthorized access to personal information.

   b. Simulate security in a Production environment.

   c. Provide object store users access to deployed objects.

   d. Prevent unauthorized access to UAT information.

3. Who has authoring rights to a solution?

   a. Anyone who is added to the project area.

   b. Anyone who is a Design object store user.

   c. Anyone who is a member of the solution architects group.

   d. Anyone who belongs to a role in the solution.

4. What does a Security Configuration package do?

   a. Simplifies security proxy configuration.

   b. Specifies security in the Development environment.

   c. Simplifies the process of applying security to production.

   d. Simplifies creating LDAP users and groups.

Answers

1. What is the main goal of security on the Development environment?

   d. Prevent unauthorized access to intellectual property.

2. What is the main goal of security on the UAT environment?

   b. Simulate security in a Production environment.

3. Who has authoring rights to a solution?

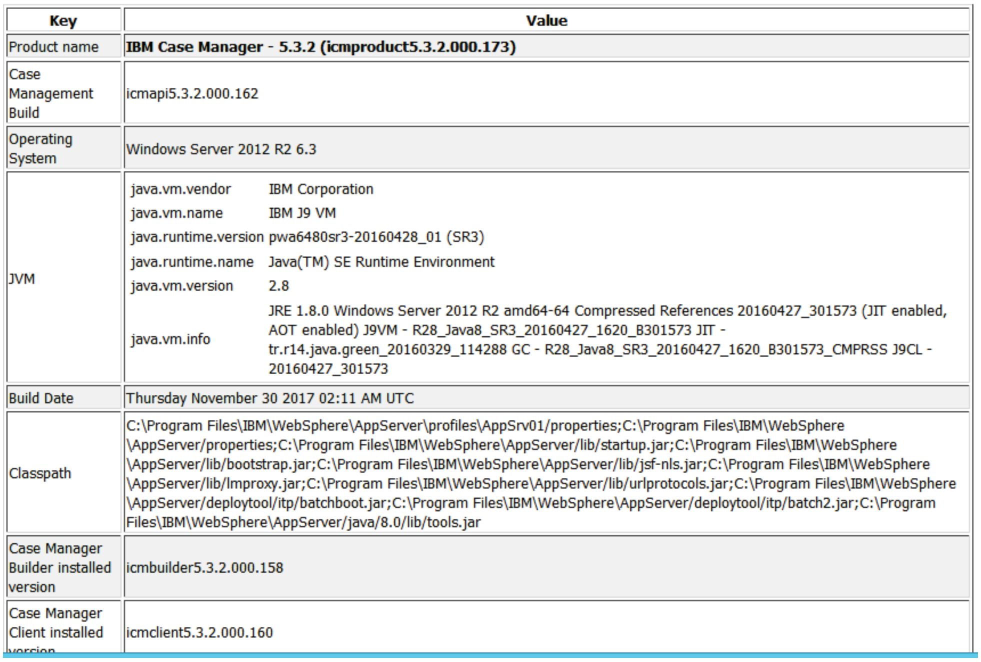
   a. Anyone who is added to the project area.

4. What does a security configuration package file do?

   c. Simplifies the process of applying security to production.

IBM Training

Demonstration 1: Start system components



Key	Value
Product name	**IBM Case Manager - 5.3.2 (icmproduct5.3.2.000.173)**
Case Management Build	icmapi5.3.2.000.162
Operating System	Windows Server 2012 R2 6.3
JVM	java.vm.vendor IBM Corporation java.vm.name IBM J9 VM java.runtime.version pwa6480sr3-20160428_01 (SR3) java.runtime.name Java(TM) SE Runtime Environment java.vm.version 2.8 java.vm.info JRE 1.8.0 Windows Server 2012 R2 amd64-64 Compressed References 20160427_301573 (JIT enabled, AOT enabled) J9VM - R28_Java8_SR3_20160427_1620_B301573 JIT - tr.r14.java.green_20160329_114288 GC - R28_Java8_SR3_20160427_1620_B301573_CMPRSS J9CL - 20160427_301573
Build Date	Thursday November 30 2017 02:11 AM UTC
Classpath	C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01/properties;C:\Program Files\IBM\WebSphere\AppServer/properties;C:\Program Files\IBM\WebSphere\AppServer/lib/startup.jar;C:\Program Files\IBM\WebSphere\AppServer/lib/bootstrap.jar;C:\Program Files\IBM\WebSphere\AppServer/lib/jsf-nls.jar;C:\Program Files\IBM\WebSphere\AppServer/lib/lmproxy.jar;C:\Program Files\IBM\WebSphere\AppServer/lib/urlprotocols.jar;C:\Program Files\IBM\WebSphere\AppServer/deploytool/itp/batchboot.jar;C:\Program Files\IBM\WebSphere\AppServer/deploytool/itp/batch2.jar;C:\Program Files\IBM\WebSphere\AppServer/java/8.0/lib/tools.jar
Case Manager Builder installed version	icmbuilder5.3.2.000.158
Case Manager Client installed version	icmclient5.3.2.000.160

Overview of security deployment

© Copyright IBM Corporation 2018

Demonstration 1: Start system components

If Case Manager is properly started, the Case Manager Ping Page resembles the screen capture.

Demonstration 1: Start system components

Purpose:
You are administering a development environment. The environment has been newly created and has not been started yet. You must start the IBM Case Manager components and then verify that the system is running.

Task1. Start IBM Case Manager components

The environment that is provided with this course requires that you start the IBM WebSphere Application servers that host the IBM Case Manager components. The WebSphere Admin folder, found on the desktop, includes the scripts that you run to start the components.

1. If your student system has recently started, wait for all automatic services to be started before you proceed.

   There are two methods to ensure that the services have started:

   - Open Task Manager and wait for CPU activity to settle to levels between 3% and 6%.
   - Open the Services manager ⚙ and wait for all of the services that start automatically to be started. In particular, the following services must be started:
   - IBM WebSphere Application Server V9.0 – Dmgr01
   - IBM WebSphere Application Server V9.0 – Node01
   - IBM WebSphere Application Server V9.0 – UATNod01
2. On the desktop, open the **WebSphere Admin** folder.
3. Right-click **_1 Start server1.bat**, and then select **Run as administrator**. Click **Yes**, and wait for the command window to close.
4. Right-click **_2 Start ICNserver.bat**, and then select **Run as administrator**, then click **Yes,** and then wait for the command window to close.

Task 2. Verify that IBM Case Manager is operational.

1. Open **Firefox**.
2. On the Course Portal Links page, under **System Health**, click **Case Manager Ping**.

3. Log in as **p8admin/FileNet1**.

   The **IBM Case Manager Context (Ping Page)** is displayed. You see a two-column table with information like: the Product name, Case Management Build version, and the Operating System.

4. Close the browser window.

Task 3. Stop and restart components (Optional)

1. If you do not see the IBM Case Manager Context (Ping Page), verify that the following two services are running:

   - **IBM WebSphere Application Server V9.0 - Dmgr**
   - **IBM WebSphere Application Server V9.0 - Node01**

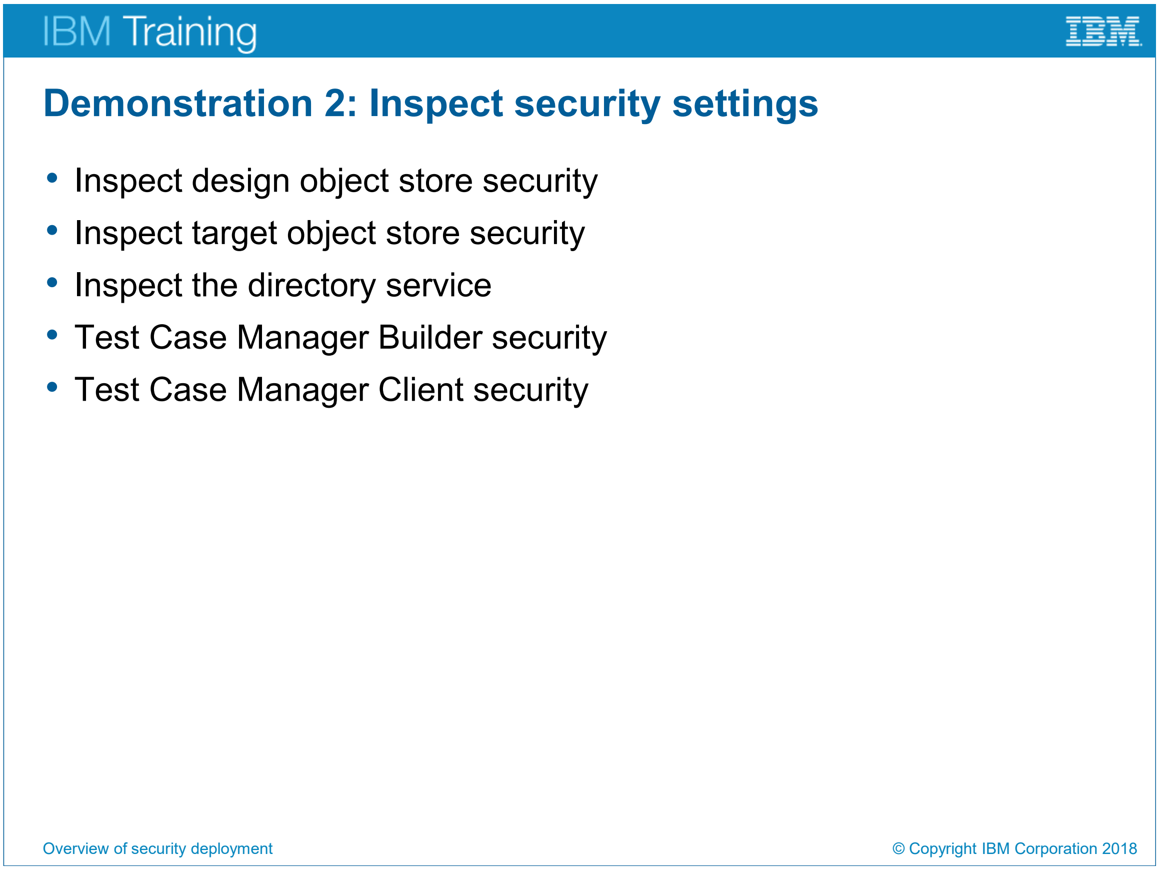
2. Stop and start the components.

   In the WebSphere Admin folder, stop the two application servers and restart them. The list of steps is:

   - Right-click **_3 Stop ICNserver.bat** and then select **Run as administrator**. Wait for the command window to close.
   - Right -click **_4 Stop server1.bat** and then select **Run as administrator**. Wait for the command window to close.
   - Right -click **_1 Start server1.bat** and then select **Run as administrator**. Wait for the command window to close.
   - Right -click **_2 Start ICNserver.bat** and then select **Run as administrator**. Wait for the command window to close.

   Do not start the next script until the command window closes for the previous script. Verify that IBM Case Manager is operational.

Results:
You started the IBM Case Manager components and confirmed that the system is running properly.



IBM Training

Demonstration 2: Inspect security settings

- Inspect design object store security
- Inspect target object store security
- Inspect the directory service
- Test Case Manager Builder security
- Test Case Manager Client security

Overview of security deployment

Demonstration 2: Inspect security settings

Demonstration 2: Inspect security settings

Purpose:
You are administering a new development system. Someone else configured system security. As a new administrator, you must familiarize yourself with the current security configurations before you change them.

Administration Console URL: **http://vclassbase:9080/acce**

Case Manager Builder URL: **http://vclassbase:9081/CaseBuilder**

User/Password: **p8admin/FileNet1**

Task 1. Inspect design object store security

Solution developers must have access to the design and target object stores. Ideally, this access is provided by group access. Identify which groups are being used to provide access to the object stores.

1. Start **Firefox**.
2. On the homepage, click the **ACCE** link to open **Administration Console for Content Platform Engine**.
3. Log on to **Administration Console for Content Platform Engine** as **p8admin/FileNet1**
4. Expand the **Object Stores** node.
5. Open the **DEV_design** object store.
6. Open the **Security** tab.
7. Verify that the following users and groups belong to the associated permission group.
    - **Case workers: Use object store**
    - **Clerks: Use object store**
    - **Solution builders: Full Control**
    - **Sysadmins: Full Control**
    - **p8admin: Full Control**
8. Close the **DEV_design** tab.

Task 2. Inspect target object store security.

1. In the navigation pane, open the **DEV_target** object store.
2. Open the **Security** tab.

3. Verify that the following users and groups belong to the associated permission group.
   - **Case workers: Use object store**
   - **Clerks: Use object store**
   - **Solution builders: Full Control**
   - **Sysadmins: Full Control**
   - **p8admin: Full Control**
4. Log out of **Administration Console for Content Platform Engine**.
5. Close **Firefox**.

Task 3. Inspect the directory service.

Your environment uses Microsoft Active Directory to provide the directory service. You know that the following groups are allowed access to the objects stores: Case workers, Clerks, Solution builders, and Sysadmins. You are going to find out who is in the Solution builders group.

1. On your desktop, click the Windows button in the toobar ⊞.
2. Click **Administrative Tools**.
3. Double-click **Active Directory Users and Computers**.
4. Scroll down until you find the **Solution builders** group.
5. Double-click the **Solution builders** group.
6. Click the **Members** tab.

   The users in this tab are currently able to use the DEV_design and DEV_target object stores.
   - Joe
   - p8admin
   - Paula
7. Click **Cancel** and then Close **Active Directory Users and Computers**.

Task 4. Test Case Manager Builder security.

1. Open **Firefox**.
2. Click the **Case Builder** link to open **Case Manager Builder**.
3. Log on to Case Manager Builder as **p8admin/FileNet1**.

4. Verify that there are no error messages and that you can see the default solution page.

   The default solution page contains the **PageBuilder** solution and the **Credit Card Dispute** solution. These are sample solutions that are not used in this course.

5. Log out of **Case Manager Builder**.

6. For each of the following accounts: log in to **Case Manager Builder**, verify access, then log out.

User name	Password	Case Manager Builder access?
Paula	FileNet1	Yes
Joe	FileNet1	Yes
Adam	FileNet1	No
Clara	FileNet1	No
Allen	FileNet1	No

   All passwords are case sensitive.

   Clara is a member of the Clerks group. Although the Clerks group has access to both object stores, Clara is unable to access Case Manager Builder. Although Clerks have object store access, they do not belong to any project area. In order to use Case Manager Builder, a user must have access to a project area.

Task 5. Test Case Manager Client security.

1. Click the Home button on the Firefox toolbar 🏠.

2. Click the **Case Client** link to open **Case Manager Client**.

3. For each of the following accounts: log in to **Case Manager Client**, verify access, then log out.

User name	**Password**	**Case Manager Client access?**
Paula	FileNet1	Yes
Adam	FileNet1	No
Clara	FileNet1	Yes
Sue	FileNet1	Yes
Allen	FileNet1	No

All passwords are case sensitive.

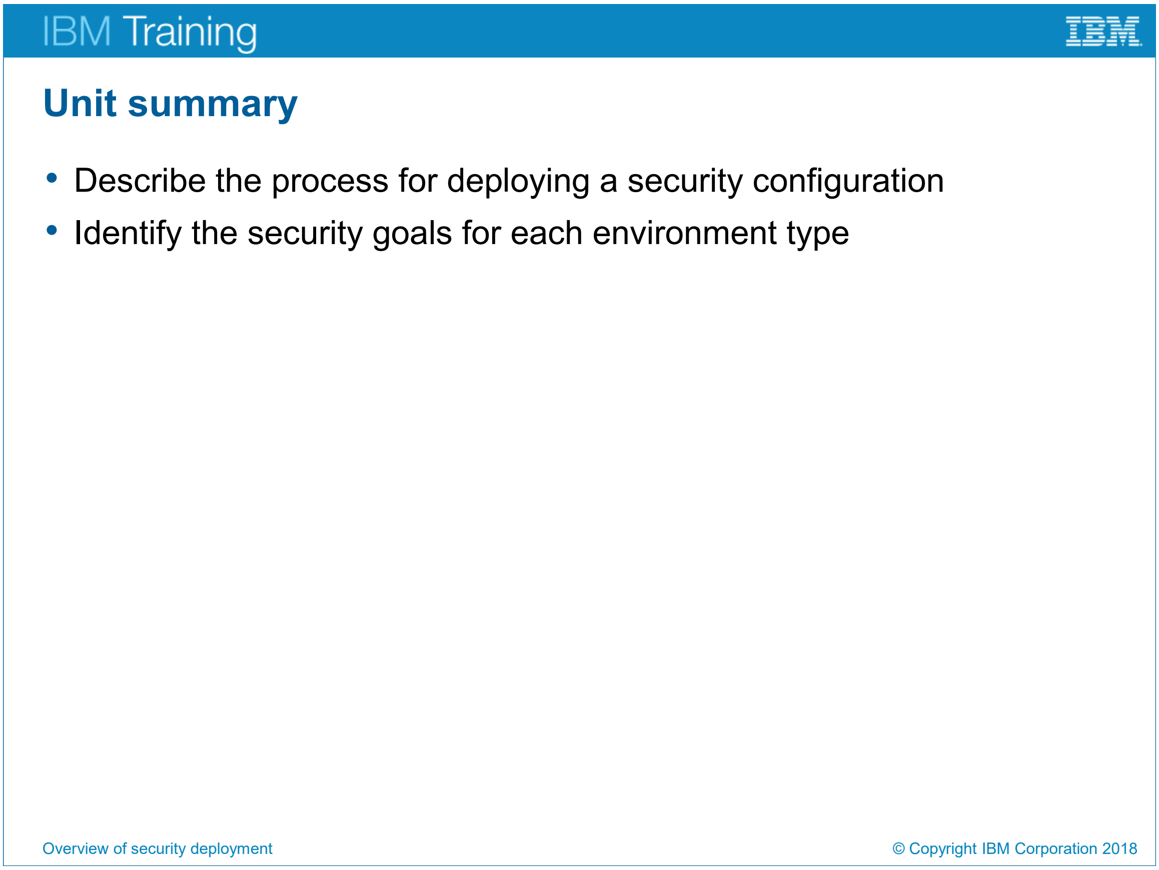
Clara is a member of the Clerks group, which has object store access.

Sue is a member of the Case Workers group, which has object store access.

Allen is a member of the Agent group, which does not have object store access.

4. Log out of any applications and close all applications and browsers.

Results:
You inspected the security configuration of the development environment.



IBM Training

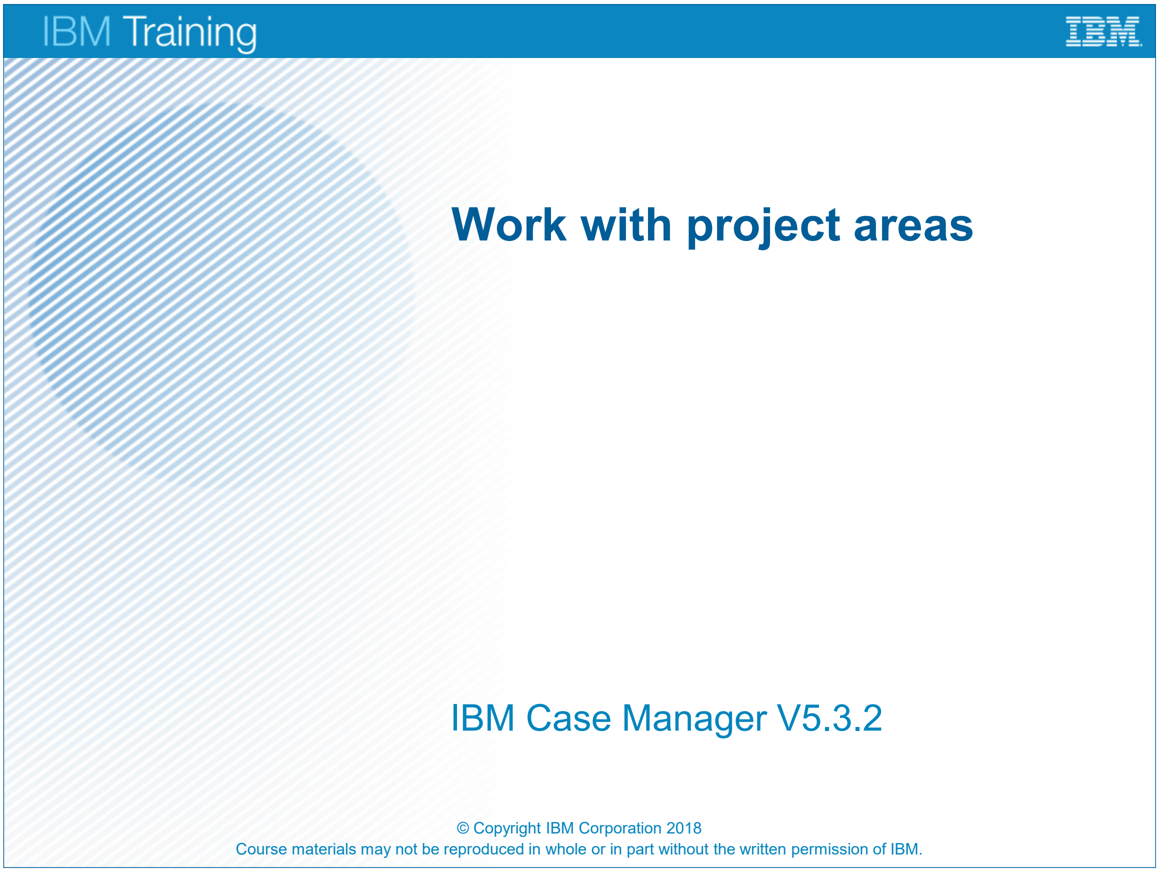
Unit summary

- Describe the process for deploying a security configuration
- Identify the security goals for each environment type

Overview of security deployment

Unit summary

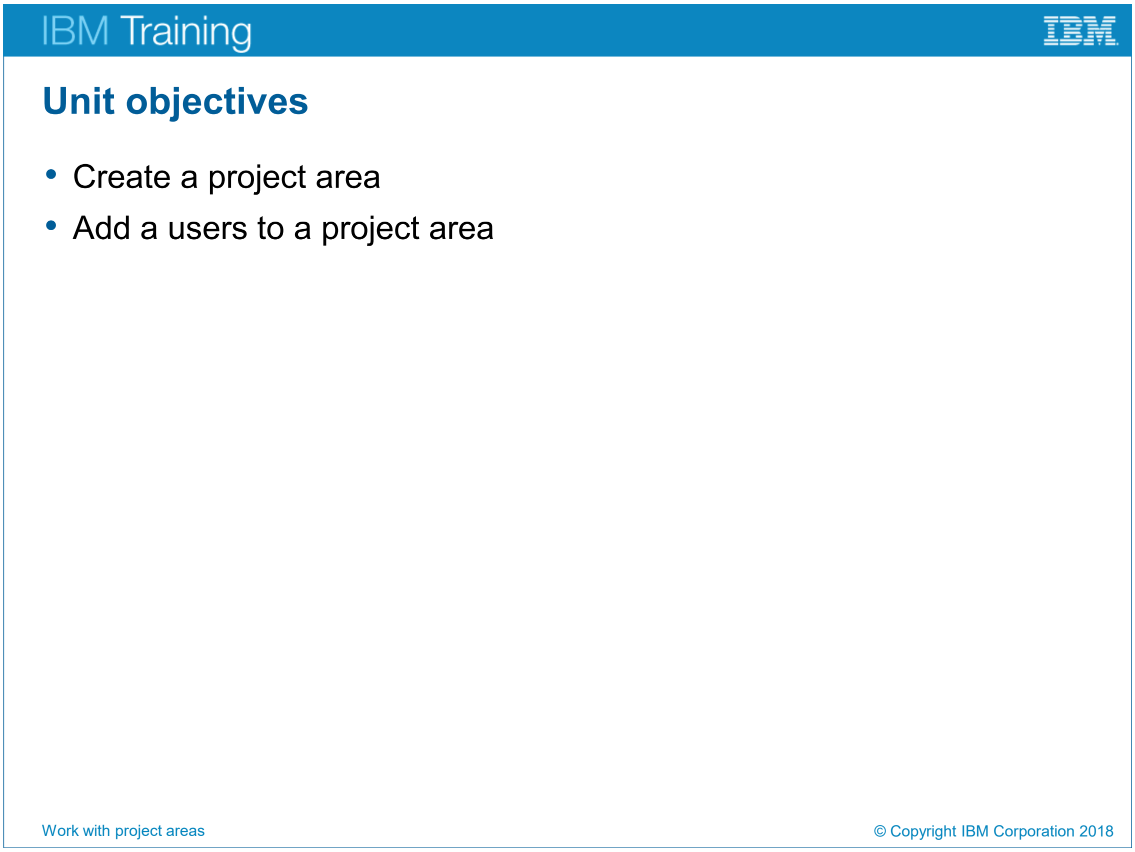
Unit 2 Work with project areas



IBM Training

Work with project areas

IBM Case Manager V5.3.2



IBM Training

Unit objectives

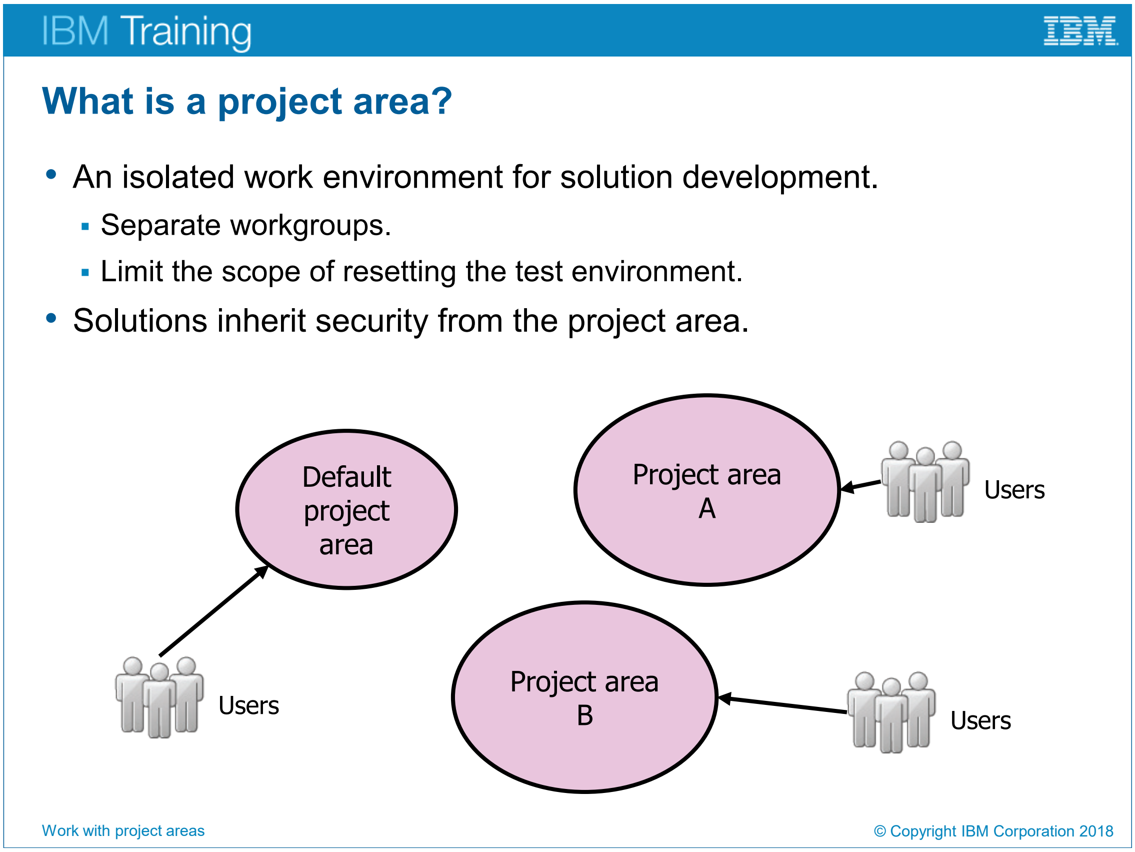
- Create a project area
- Add a users to a project area

Work with project areas

© Copyright IBM Corporation 2018

Unit objectives

You need to add users to a project area so that they can work on building solutions in the Development environment.



IBM Training

What is a project area?

- An isolated work environment for solution development.
  - Separate workgroups.
  - Limit the scope of resetting the test environment.
- Solutions inherit security from the project area.

Work with project areas

© Copyright IBM Corporation 2018

What is a project area?

A system administrator configures project areas for solution architects and business analysts.

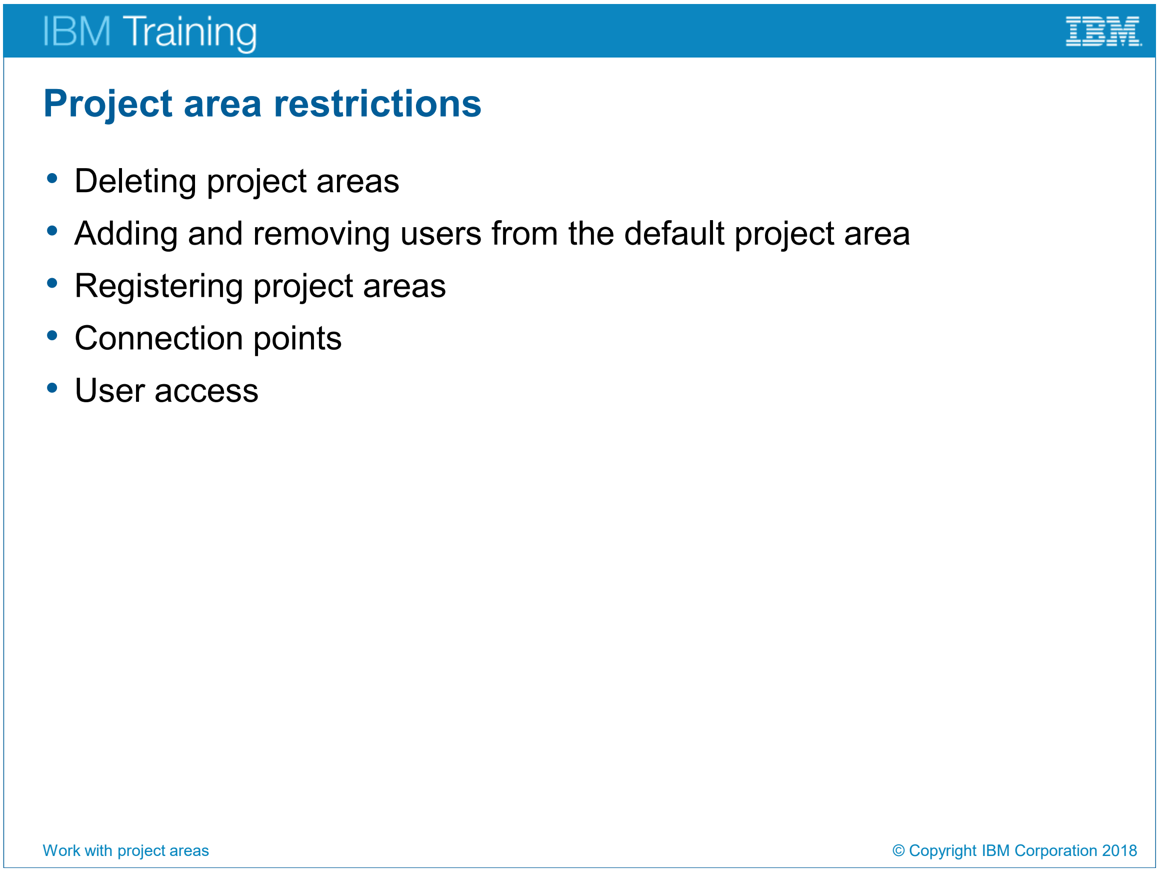
A project area is an isolated work environment for solution development. A design object store can have one or more project areas. Project areas isolate work so that different teams can work independently on solution designs.

If you reset the test environment for one project area, no other project areas are affected.

Each development environment has a default project area named dev_env_connection_definition. If you create more project areas, you must specify users who have access to them. A user can access only one assigned project area in addition to the default project area.

All solutions inherit security from the project area.

If you add a user to a project area, that user has access to the solutions within the project area.



IBM Training

Project area restrictions

- Deleting project areas
- Adding and removing users from the default project area
- Registering project areas
- Connection points
- User access

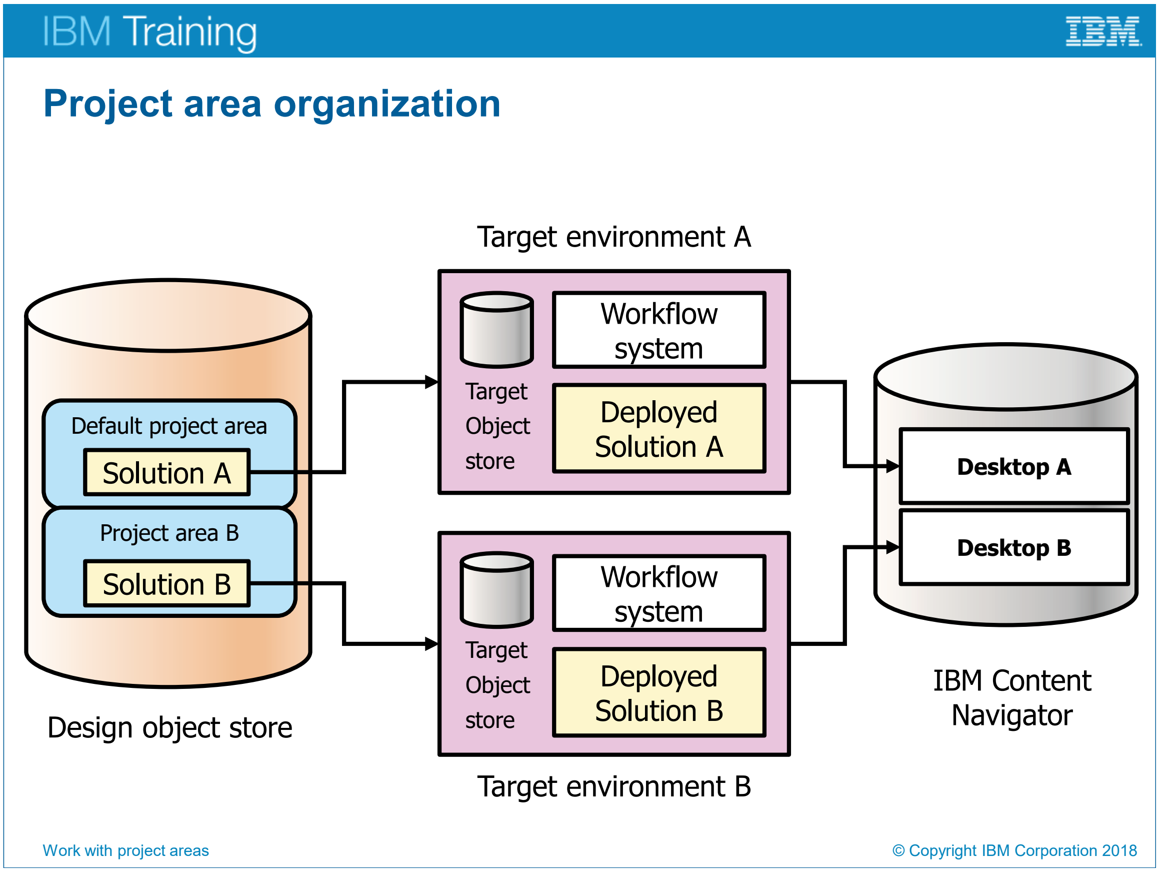
Work with project areas

© Copyright IBM Corporation 2018

Project area restrictions

The following restrictions apply to project areas:

- You cannot delete the default project area; you can delete regular project areas only.
- You can add and remove users and groups from the default project area. For regular project areas, you can add and remove individual users only.
- Each project area must have at least one assigned user.
- After you define a project area, you must register it before you can use it.
- Each project area requires a unique connection point, and only one connection point can be associated with a target object store.
- You can add a user to one regular project area only, in addition to the default project area. If you provide a user access to both default and regular project areas, the user can access only the regular project area.



IBM Training

Project area organization

Target environment A

Design object store

Default project area

Solution A

Project area B

Solution B

Target Object store

Workflow system

Deployed Solution A

Target Object store

Workflow system

Deployed Solution B

Target environment B

Desktop A

Desktop B

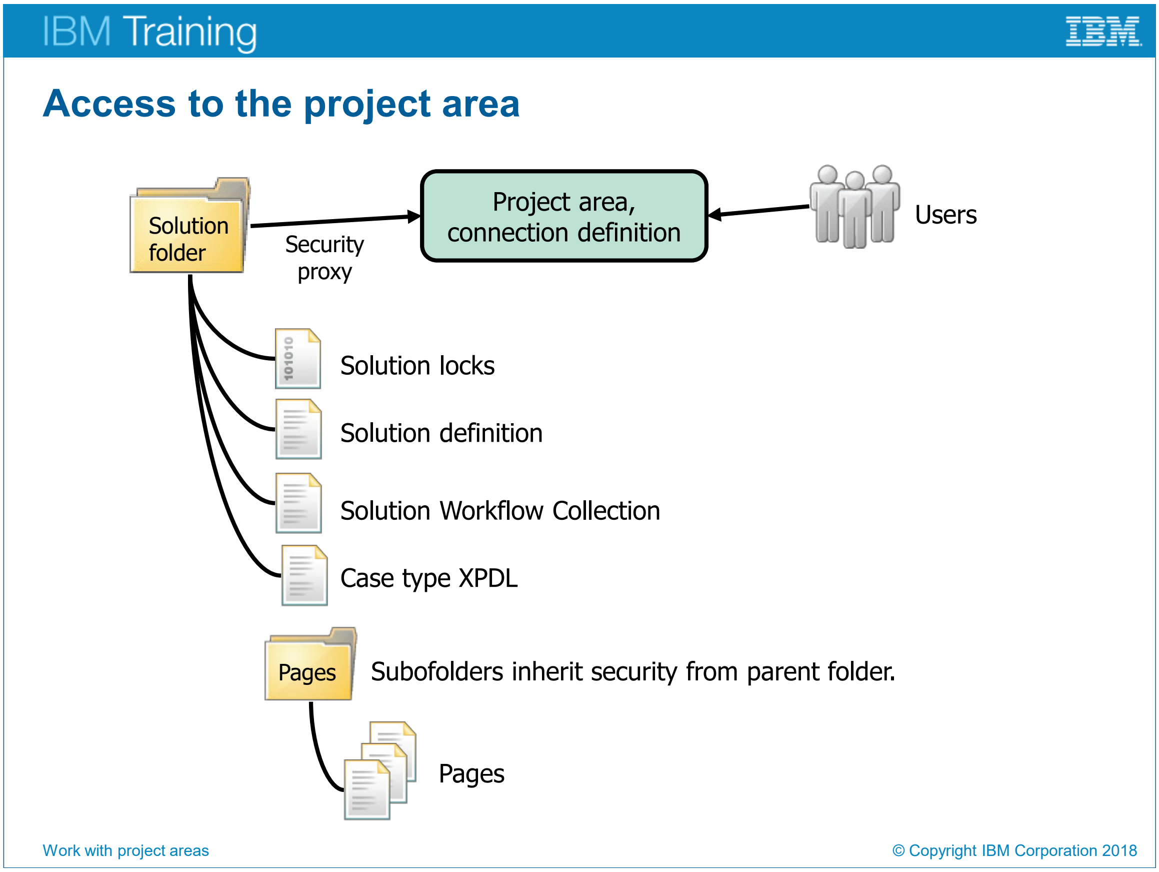
IBM Content Navigator

Work with project areas

© Copyright IBM Corporation 2018

Project area organization

The graphic shows how project areas correspond to object stores and workflow systems.



IBM Training

Access to the project area

Solution folder

Security proxy

Project area, connection definition

Users

Solution locks

Solution definition

Solution Workflow Collection

Case type XPDL

Pages

Subofolders inherit security from parent folder.

Pages

Work with project areas

© Copyright IBM Corporation 2018

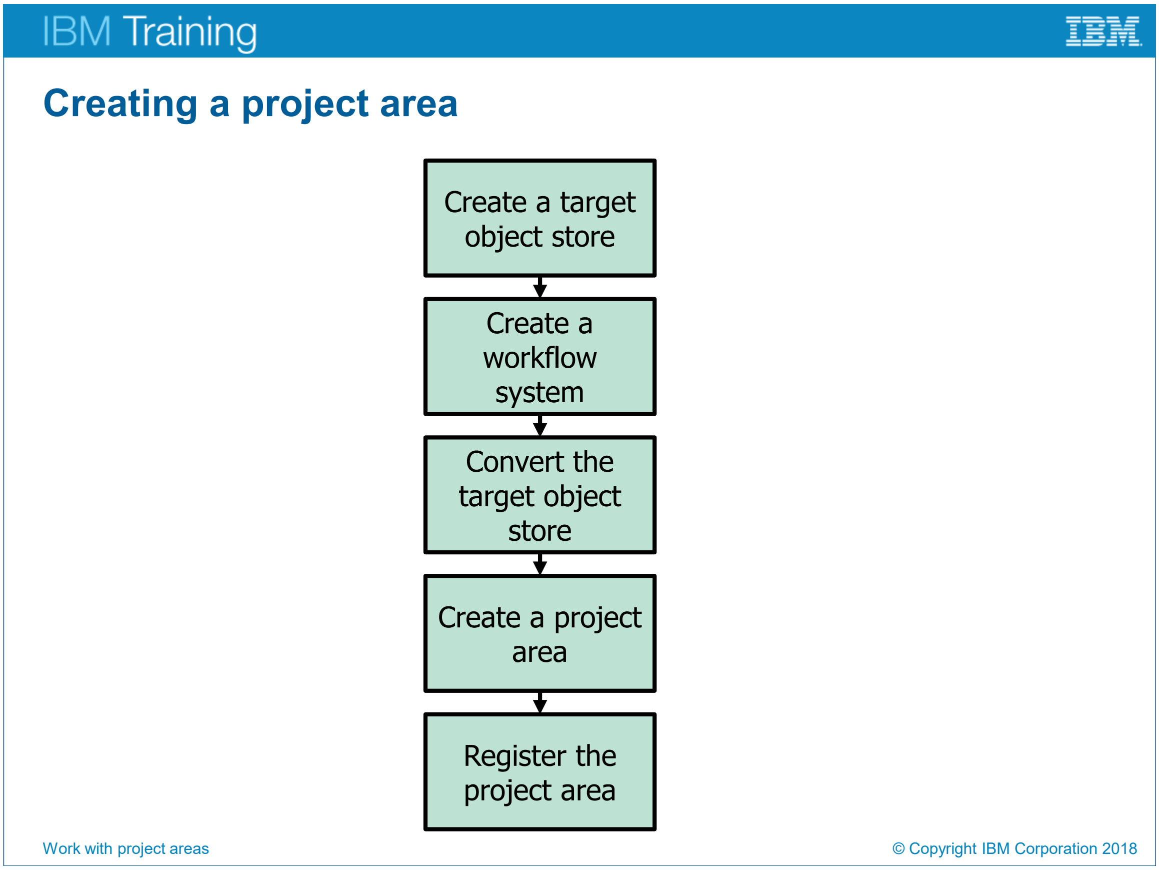
Access to the project area

Within the project area, users have access to the solution folder. Solution folders provide access to all subfolders and objects, such as the solution definition and case type files.

Solution locks prevent solution builders from overwriting one another’s work. When you are working on a solution artifact, other users are prevented from editing that artifact.

If a user belongs to the object store security group that has access to the default project area, that user can access the default project area. However, if that user is added to another project area, then that user automatically only sees the other project area after logging on to Case Manager Builder.

A user can belong to the default project area plus one other project area.



IBM Training

Creating a project area

Create a target object store

Create a workflow system

Convert the target object store

Create a project area

Register the project area

Work with project areas

© Copyright IBM Corporation 2018

Creating a project area

Each project area requires a separate connection point. Each connection point requires a workflow system. Each workflow system requires an object store. So, before you can create a project area, you must create a target object store and then create a workflow system. When you define the workflow system, you create a workflow isolated region and a connection point.

When you create the object store, remember the following requirements:

- You must configure the object store as an IBM Case Manager target object store. Select the appropriate add-ons, and also run the convert object store task from the IBM Case Manager configuration tool.
- You can use the same database as other object stores, but you must choose a new schema name.
- Provide solution architects group full control over the object store.
- Provide tester groups (if any) with use object store access.

When you create the workflow system, remember the following requirements:

- You can use an existing database table.
- You must specify a new isolated region name and number.

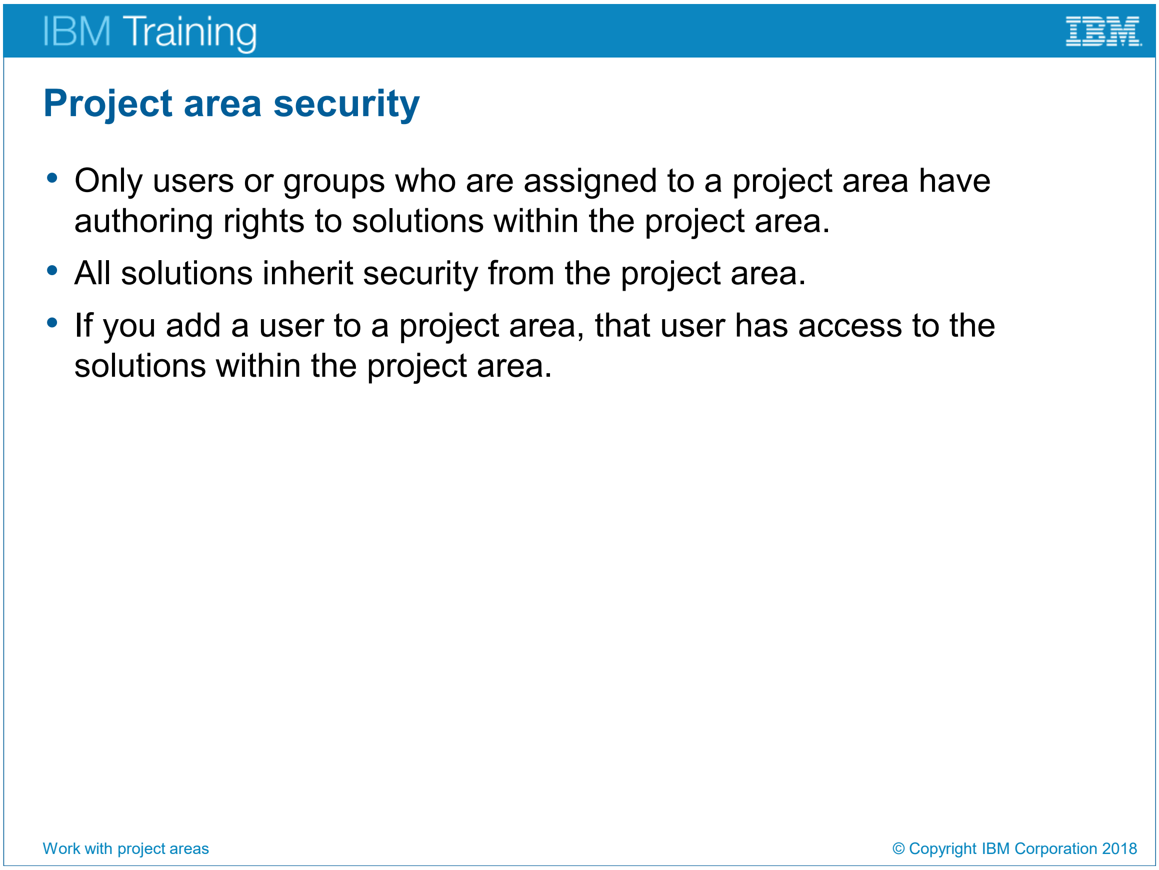
When you convert the object store to a target object store, remember to use *IBM Case Manager configuration tool*. Do not confuse this tool with *IBM FileNet Configuration Manager* or *IBM Content Navigator Configuration and Deployment tool*. All three tools have the same filename (configmgr.exe) but are distinguished by their file locations.

When you create the project area, remember the following requirements:

- Use IBM Case Manager Administration Client.
- Project areas are defined from the design object store.
- The object store and connection point must already be defined.
- Be prepared to add users to the project area.

You can register the project area by using either *IBM Case Manager Administration client*, or *IBM Case Manager configuration tool*. The results are the same, however, the potential issues are different:

- IBM Case Manager Administration client is an EJB application in WebSphere. WebSphere-related problems can cause failure.
- IBM Case Manager configuration tool is a stand-alone java application. JRE-related issues can cause failure.



IBM Training

Project area security

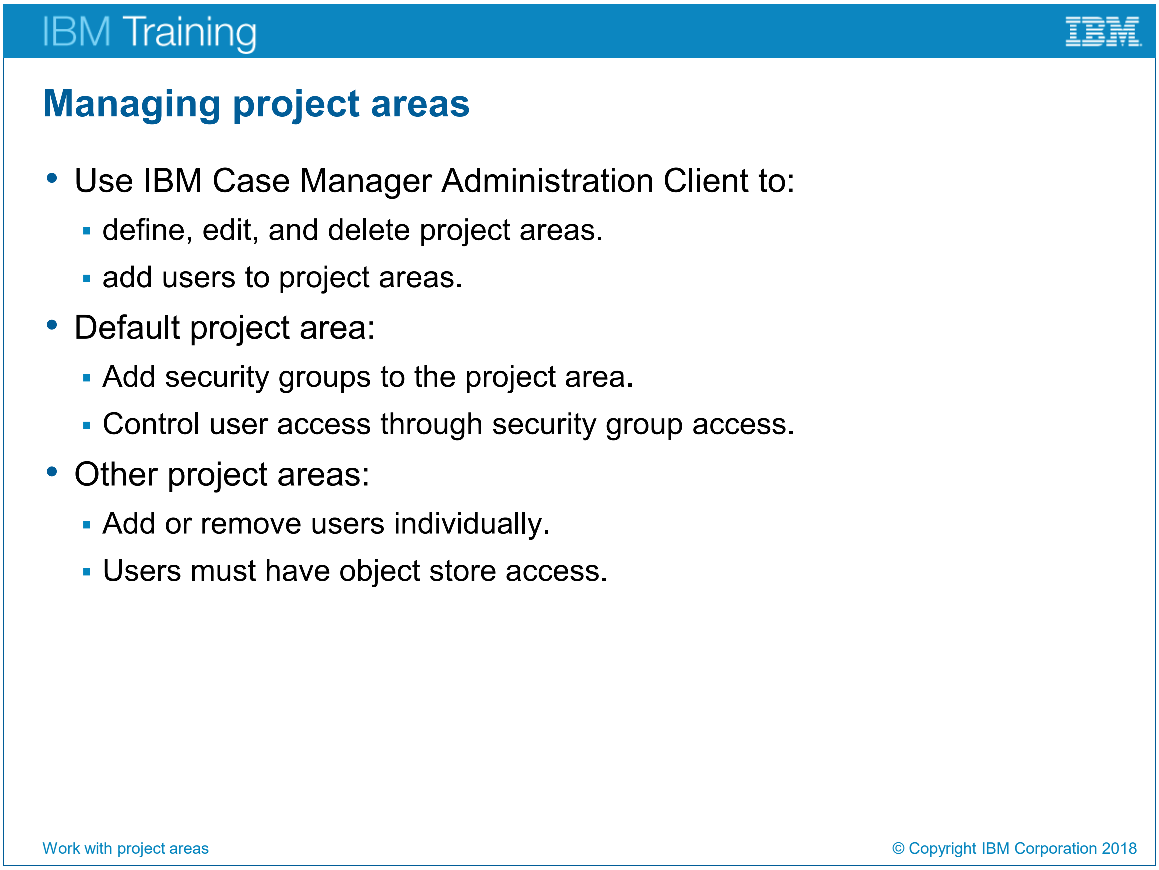
- Only users or groups who are assigned to a project area have authoring rights to solutions within the project area.
- All solutions inherit security from the project area.
- If you add a user to a project area, that user has access to the solutions within the project area.

Work with project areas

© Copyright IBM Corporation 2018

Project area security

When creating the target object store, you must add users or groups to the administration group for the target object store so that in the IBM Case Manager administration client you can add the users to a project area. To initiate a test environment reset, a user must have system administrator privileges on the target object store.



IBM Training

Managing project areas

- Use IBM Case Manager Administration Client to:
  - define, edit, and delete project areas.
  - add users to project areas.
- Default project area:
  - Add security groups to the project area.
  - Control user access through security group access.
- Other project areas:
  - Add or remove users individually.
  - Users must have object store access.

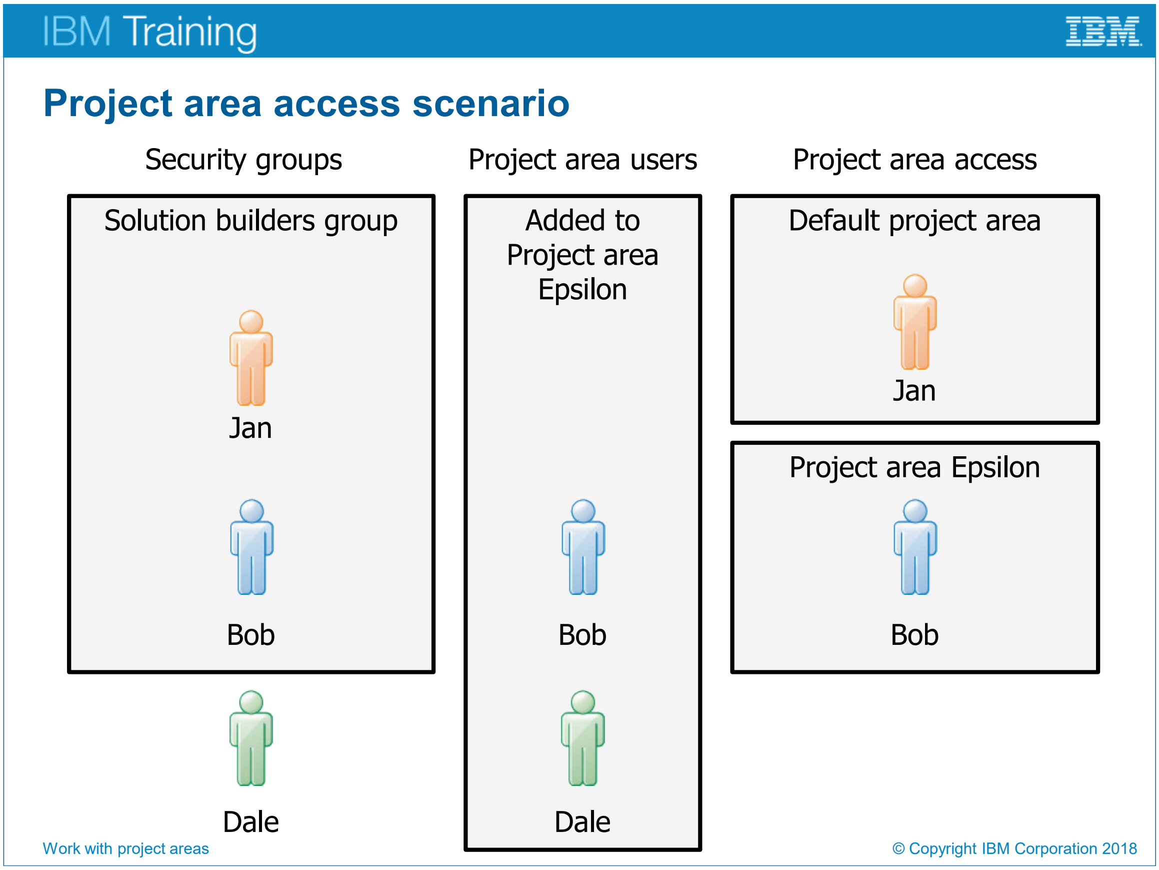
Work with project areas

© Copyright IBM Corporation 2018

Managing project areas

By default, an IBM Case Manager development environment includes a default project area. The default project area is different from other project areas. You can add security groups to the default project area, but you can add only individuals to other project areas. When you create the target object store, you define groups that have administrative rights to the object store. It is useful to add one of these groups to the default project area. After that, you can control access to the default project area by controlling who is in the group. You must add at least one user to the default project area before you can use Case Manager Builder.

You cannot add groups to non-default project areas. You must add users individually. A user must still have access to the design and target object stores. Control the object store access by using security groups, then add the users to the project area individually.



IBM Training

Project area access scenario

Security groups

Solution builders group

Jan

Bob

Dale

Project area users

Added to Project area Epsilon

Bob

Dale

Project area access

Default project area

Jan

Project area Epsilon

Bob

Work with project areas

© Copyright IBM Corporation 2018

Project area access scenario

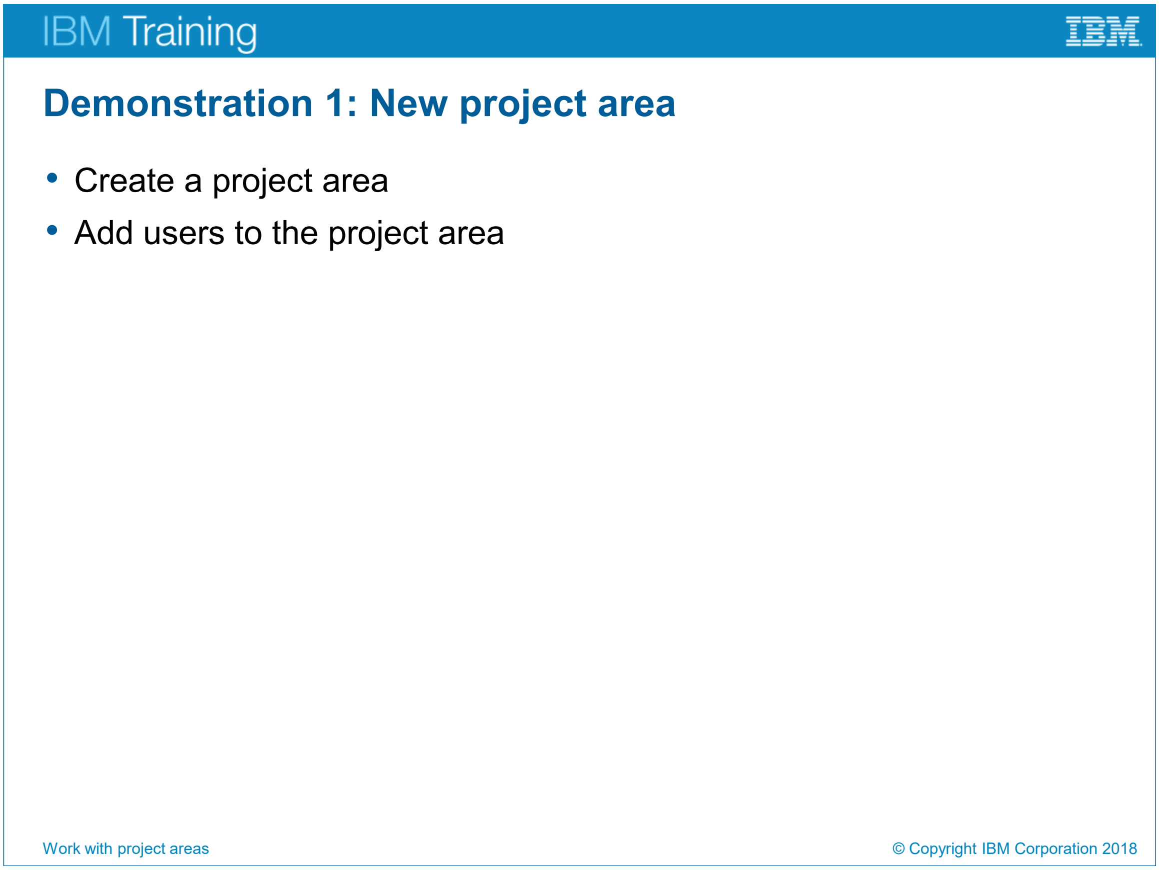
The scenario in the graphic illustrates how project area access is applied. Jan, Bob, and Dale are all employees at a company. Jan and Bob are members of the Solution builders group, which has full access to the design and target object stores. Dale is not a member of this group, but is an authenticated user at the company.

The Solution builders group was added to the default project area.

Bob and Dale were added to Project area Epsilon.

The result is that Jan has access to the default project area. Bob has access only to project area Epsilon because users can see only one project area per logon. Dale has no access, because he cannot access the object stores, even though Dale was added to the project area.

The administrator should either add Dale to the Solution builders group or remove him from the project area.



IBM Training

Demonstration 1: New project area

- Create a project area
- Add users to the project area

Work with project areas

Demonstration 1: New project area

Demonstration 1: New project area

Purpose:
You are the administrator for an IBM Case Manager system. A new team of developers need to start working in their own project area. You need to create the project area for them.

Administration Console for Content Platform Engine URL:
http://vclassbase:9080/acce

Case Manager Builder URL: **http://vclassbase:9081/CaseBuilder**

ICM Admin Client: **http://vclassbase:9081/navigator/?desktop=icmadmin**

Administrator Username:	**p8admin**
Administrator Password:	**FileNet1**

Task 1. Create an object store.

1. Start **Firefox.**
2. Click the **ACCE** link on the homepage to open **Administration Console for Content Platform Engine**, and then log in as **p8admin/FileNet1.**
3. Select **Object Stores**, then click **New**.
4. Complete the **Name the object store** page:
   a. In the Display Name field, type `DEV_Target_2`.
   b. Click **Next**.
5. On the **Define the database** page, complete the following steps:
   - Select a **Database connection**: **ICMDBDS**.
   - In the **Schema name** field, type `dev2`.
   - Click **Next**.
6. Click **Next** on the **Select the Type of Storage Area for Content** page.
7. On the **Grant Administrative Access** page, complete the following steps:
   - Click **Add User/Group Permission**.
   - Search for and then add the **Solution builders** group.
   - Click **OK**.

   You might need to scroll down to see the **OK** button.

   - Click **Next**.

8. On the **Grant Basic Access** page, complete the following steps:
   - Click **Add User/Group Permission**.
   - Add **Clerks** and **Case workers**.
   - Click **OK**
   - Click **Next**.
9. On the **Select Add-ons** page, complete the following steps:
   - Click **Workplace/Workplace XT Configuration**.

     .
   - Click **Next**.

   Although you do not use Workplace or Workplace XT for IBM Case Manager, this button simplifies the task of selecting the prerequisite standard add-ons that are needed to run IBM Case Manager solutions.
10. Click **Finish** and wait for the process to complete.

    If you did not select all of the correct add-ons, you can add them with Administration Console by right-clicking the object store and selecting *Install Add-ons Features*.

Task 2. Create a workflow system.

1. In **Administration Console for Content Platform Engine**, open **DEV_Target_2**.
2. Open **Administrative**.
3. Right-click **Workflow System** > Click **New**.
4. On the **New Workflow System** page, complete the following steps:
   - In the **Data** field, type `DEV`.

   DEV is the name of the existing tablespace. You can create a new tablespace to keep work separate.
   - For **Administration group**, click **Browse**.
   - Add **Solution builders**, then click **OK**.
   - Click **Next**.

5. Complete the **Specify New Connection Point** page:
   - In the **Connection point name** field, type `DEV2targetCP33`.

   Provide meaningful names for your connection points. This connection point is for the Dev2 target object store and uses the isolated region number 33.

   - Click **Next**.
6. On the **Specify New Isolated Region** page, enter the following data, then click **Next**.
   - **Isolated region name**: `DEV2targetRegion`
   - **Isolated region number**: `33`
7. Click **Next** on the **Specify Isolated Region Table Space (optional)** page.
8. Click **Finish** on the **Summary** page and wait for the process to complete.
9. Click **Close**.
10. Log out of **Administration Console for Content Platform Engine** and Close **Firefox**.

Task 3. Convert the object store into a target object store.

1. Browse to C:\IBM\CaseManagement\configure.
2. Right-click **configmgr.exe** and click **Run as Administrator**.
3. Open the configuration profile:
   - Click **File** > **Open Profile**.
   - Browse to **C:\IBM\FileNetP8\config\ICM532-config**.
   - Select **ICM532-config.cfgp**.
   - Click **Open**.
4. Expand the profile to view the tasks.
5. Double-click the **Configure the Case Management Object Stores** task.
6. In the **Display name for the target object store** field, select **DEV_Target_2**.
7. Click **Save**.
8. Click **Run Task**.
9. Wait for the task to complete.
10. Minimize **IBM Case Manager configuration tool**.

    You use this tool again to register your project area.

Task 4. Create a project area.

1. Start **Firefox**.
2. From the home page, click the **Case Admin** link to open **Case Manager Admininistration Client**.
3. Log in as **p8admin/FileNet1**.
4. Click **DEV_design**.
5. Click **Project Areas**.
6. Click **Define**.
7. On the **Define the project area properties** page, complete the following steps:
   - In the **Project area name** field, type `Project_2`.
   - On the **Connection Point** menu, select **DEV2targetCP33**.
   - Click **Next**.
8. Click **Next** on the **Add solutions to the project area** page.
9. On the **Add users to the project area** page, add **Paula**, then click **Next**.
10. Review your settings and then click **Finish**.
11. Click **Close** and then log out of **Case Manager Administration Client**.

Task 5. Register the project area.

1. Restore **IBM Case Manager configuration tool**.
2. Open the task: **Register Project Area**.
3. Select **Project_2** from the **Project Area** field.
4. Click **Save**.
5. Click **Test Connection** and click **OK** to close the success message.
6. Click **Run Task**.
7. Wait for the task to finish, then close **IBM Case Manager configuration tool**.

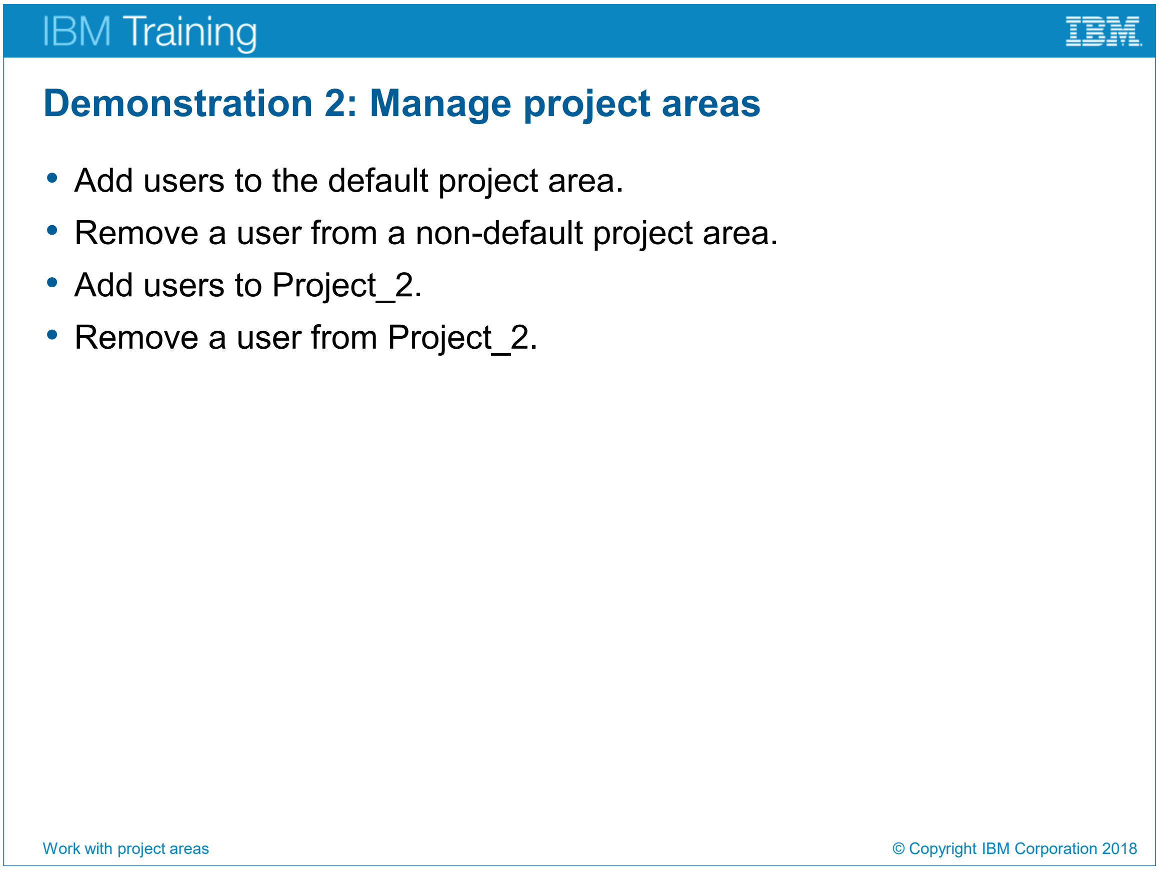
Task 6. Test the project area.

1. Log in to **Case Manager Builder** as **Joe/FileNet1**.
2. Verify that you can see the **PageBuilder** and **Credit Card Dispute** solutions, then log out.

   These solutions exist on the default project area.
3. Log in to **Case Manager Builder** as **Paula/FileNet1.**
4. Verify that there are no solutions in the solutions page.

5. Create a simple solution with the following values:
   - **Solution name**: `Test solution`
   - **Solution prefix**: `TEST`
   - **String property**: `Test property`
   - **Role**: `Tester`
   - **Case type:** `Test case`
6. Deploy the solution.
7. Confirm that the solution deploys without errors ✓.
8. Click **Actions** ⋮ > **Remove** to remove the solution.
9. Log out of all applications and close all browsers.

Results:
You created a project area and added users to it.



IBM Training

Demonstration 2: Manage project areas

- Add users to the default project area.
- Remove a user from a non-default project area.
- Add users to Project_2.
- Remove a user from Project_2.

Work with project areas

© Copyright IBM Corporation 2018

Demonstration 2: Manage project areas

Demonstration 2: Manage project areas

Purpose:
The default project area can be managed with groups. There is a user who needs access to the default project area. You are going to add this user to the default project area by editing the Solution builders group. Other users need access to Project_2. You add these users individually.

Task 1. Add a user to the default project area.

1. On your desktop, click the Windows button in the toobar ⊞.
2. Click **Administrative Tools**, then double-click **Active Directory Users and Computers**.
3. Scroll down until you find the **Solution builders** group, then double-click **Solution builders**.
4. Open the **Members** tab.
5. Click **Add**.
6. Type `Vinny`, then click **Check Names**. Click **OK**.
7. Add **Adam** and **Allen** to the **Solution builders** group.
8. Click **OK** to close the **Solution builders** window.
9. Close **Active Directory Users and Computers**.

Task 2. Test Case Manager Builder access.

1. Start **Firefox**.
2. Log in to **Case Manager Builder** as **Vinny/FileNet1**.
3. Verify that **Vinny** has access to the solutions in the default project area, then log out.

   The default project area contains the **PageBuilder** and **Credit Card Dispute** solutions.
4. Log in to **Case Manager Builder** as **Adam/FileNet1**.
5. Verify that **Adam** has access to the solutions in the default project area, then log out.
6. Log in to **Case Manager Builder** as **Allen/FileNet1**.
7. Verify that **Allen** has access to the solutions in the default project area, then log out.

Task 3. Add users to the Project_2 project area.

1. In **Firefox**, log in to **Case Manager Administration Client** as **p8admin/FileNet1**.
2. Open the **DEV_design** object store.
3. Expand **Project Areas**.
4. Open **Project_2**.
5. Open the **Security** tab.
6. Click **Add**.
7. Add **Adam** and **Allen** to the project area.
8. Click **Finish**.
9. Wait for the operation to complete, then log out of **Case Manager Administration Client**.

Task 4. Test Project_2 access.

1. Log in to **Case Manager Builder** as **Adam/FileNet1**.
2. Verify that **Adam** has access to the Project_2 project area, then log out.

   This project area has no solutions.
3. Log in to **Case Manager Builder** as **Allen/FileNet1**.
4. Verify that **Allen** has access to the Project_2 project area, then log out.

Task 5. Remove a user from the Project_2 project area.

1. Log in to **Case Manager Administration Client** as **p8admin/FileNet1**.
2. Open the **DEV_design** object store.
3. Expand **Project Areas**.
4. Open **Project_2**.
5. Open the **Security** tab.
6. Select **Allen**.
7. Click **Remove**.
8. Click **Finish**.
9. Wait for the operation to complete, then log out of **Case Manager Administration Client**.

Task 6. Test Project_2 access.

1. Log in to **Case Manager Builder** as **Allen/FileNet1**.
2. Verify that **Allen** has access to the default project area, then log out.

   The **PageBuilder** and **Credit Card Dispute** solutions are visible in the default project area.

Task 7. Remove a user from the default project area.

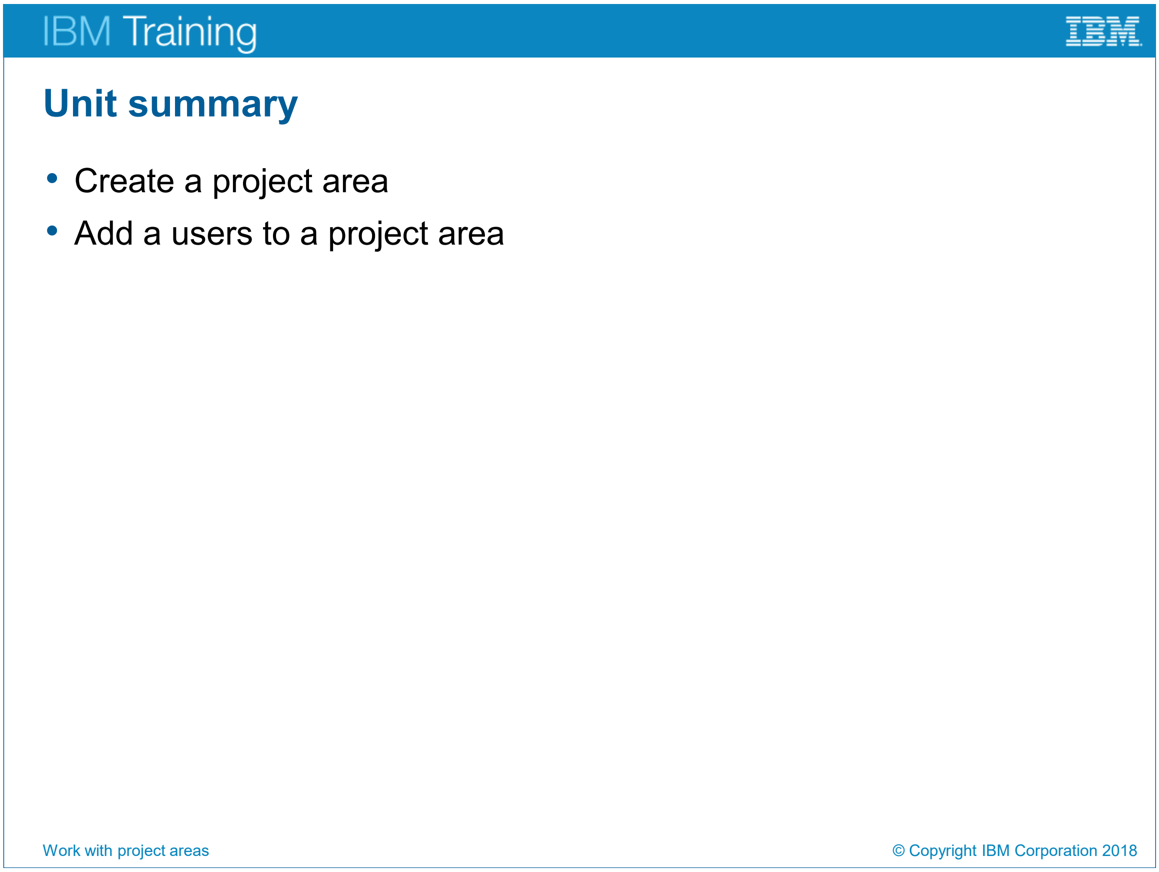
1. Open **Active Directory Users and Computers**.
2. Scroll down until you find the **Solution builders** group.
3. Double-click **Solution builders**.
4. Open the **Members** tab.
5. Select **Allen**.
6. Click **Remove**, then click **OK**.
7. Close **Active Directory Users and Computers**.

Task 6. Test default project area access.

1. Log in to **Case Manager Builder** as **Allen/FileNet1**.
2. Verify that Allen has no access to the default project area, then log out.
3. Close all applications and log out of all browsers.

Result:

You added users to project areas to provide access to solutions. You removed users from project areas to restrict access to solutions.



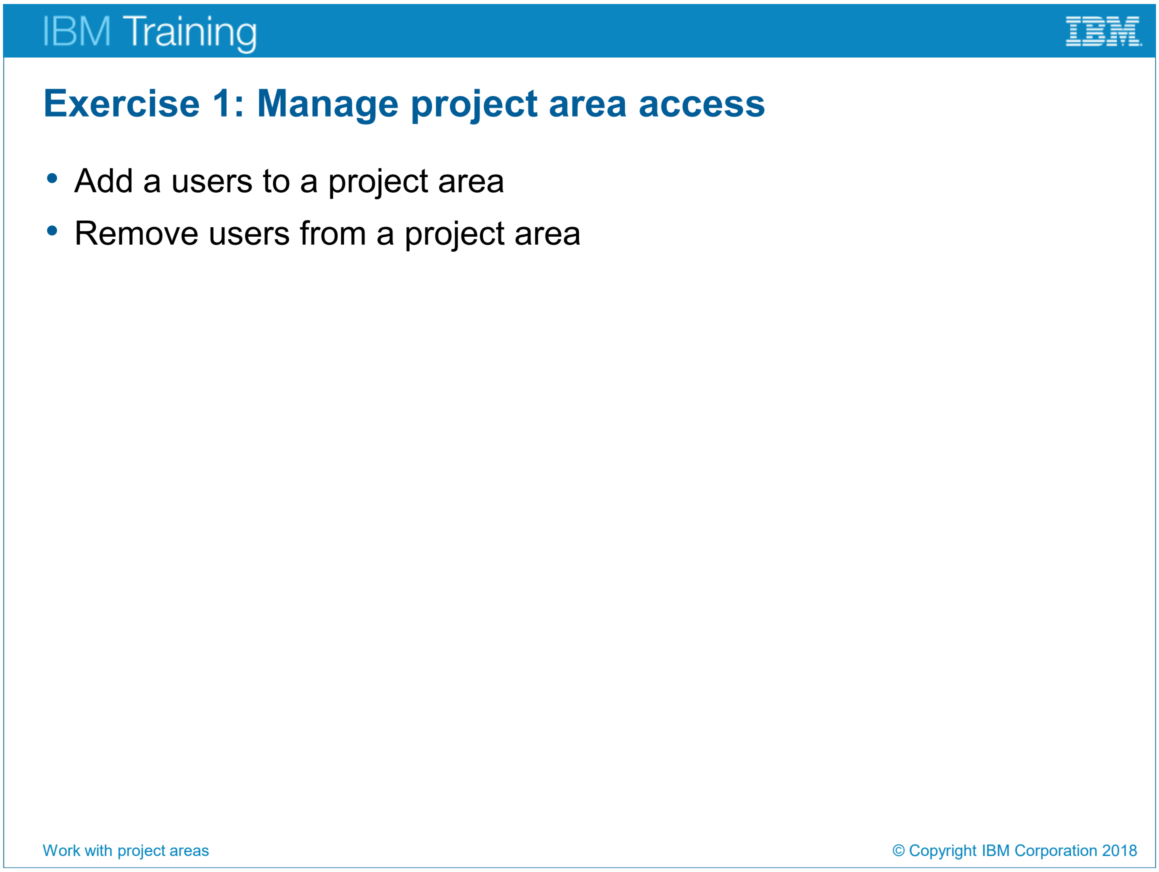
IBM Training

Unit summary

- Create a project area
- Add a users to a project area

Work with project areas

Unit summary



IBM Training

Exercise 1: Manage project area access

- Add a users to a project area
- Remove users from a project area

Work with project areas

© Copyright IBM Corporation 2018

Exercise 1: Manage project area access

Exercise 1:
Manage project area access

You are managing development environments for solution builders. The company has hired two new solution builders. One of the solution builders needs to be added to the default project area. The other solution builder must be added to the Project_2 project area.

- Add **Burt** to the Project_2 project area.
- Add **Carol** to the default project area.
- Verify user access.

For more information about where to work and the exercise results, refer to the Tasks and Results section that follows. If you need more information to complete a task, refer to earlier demonstrations for detailed steps.

Exercise 1:
Tasks and results

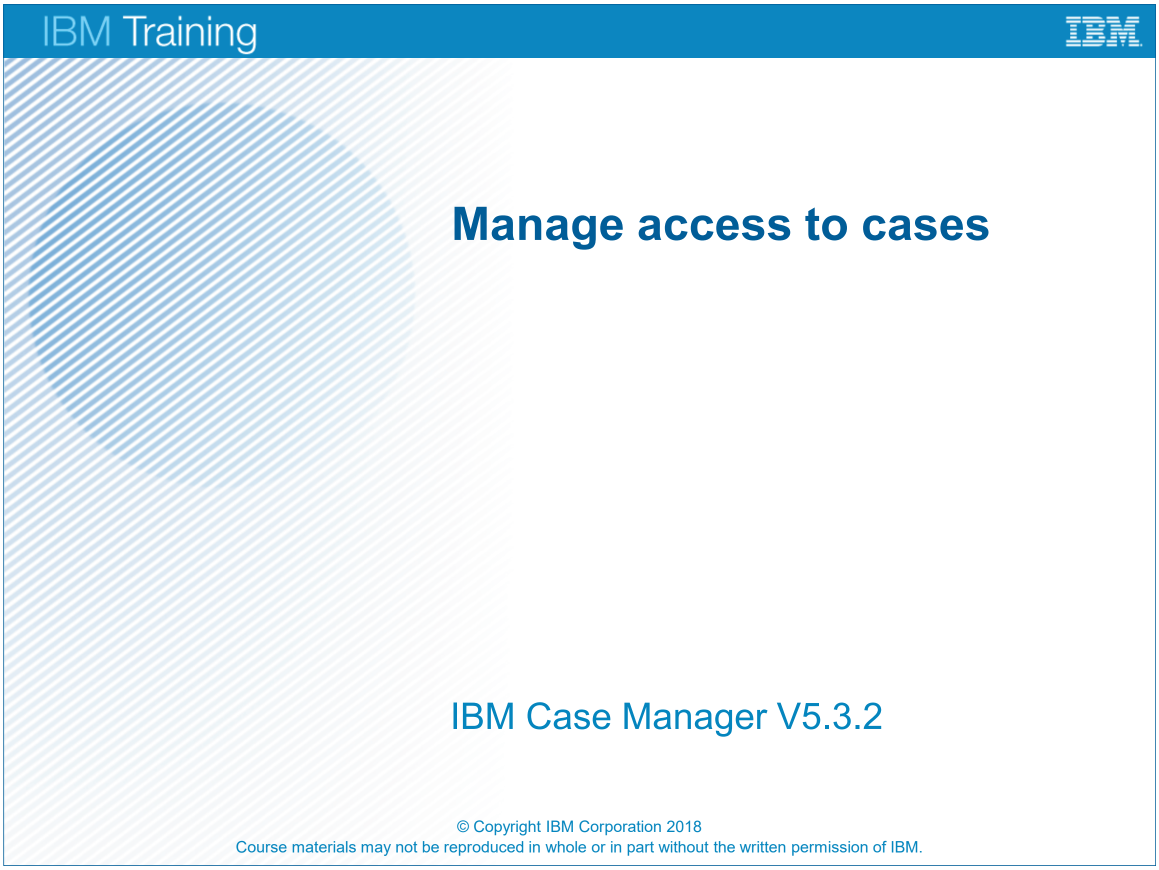
Task 1. Add Burt and Carol to the Solution builders group.

- Add **Burt** and **Carol** to the **Solution builders** group.
- Verify that **Burt** and **Carol** can access the default project area.

Task 2. Add Burt to the Project_2 project area.

- Add Burt to the **Project_2** project area.
- Verify that **Burt** can access the **Project_2** project area.
- Log out and close all applications.

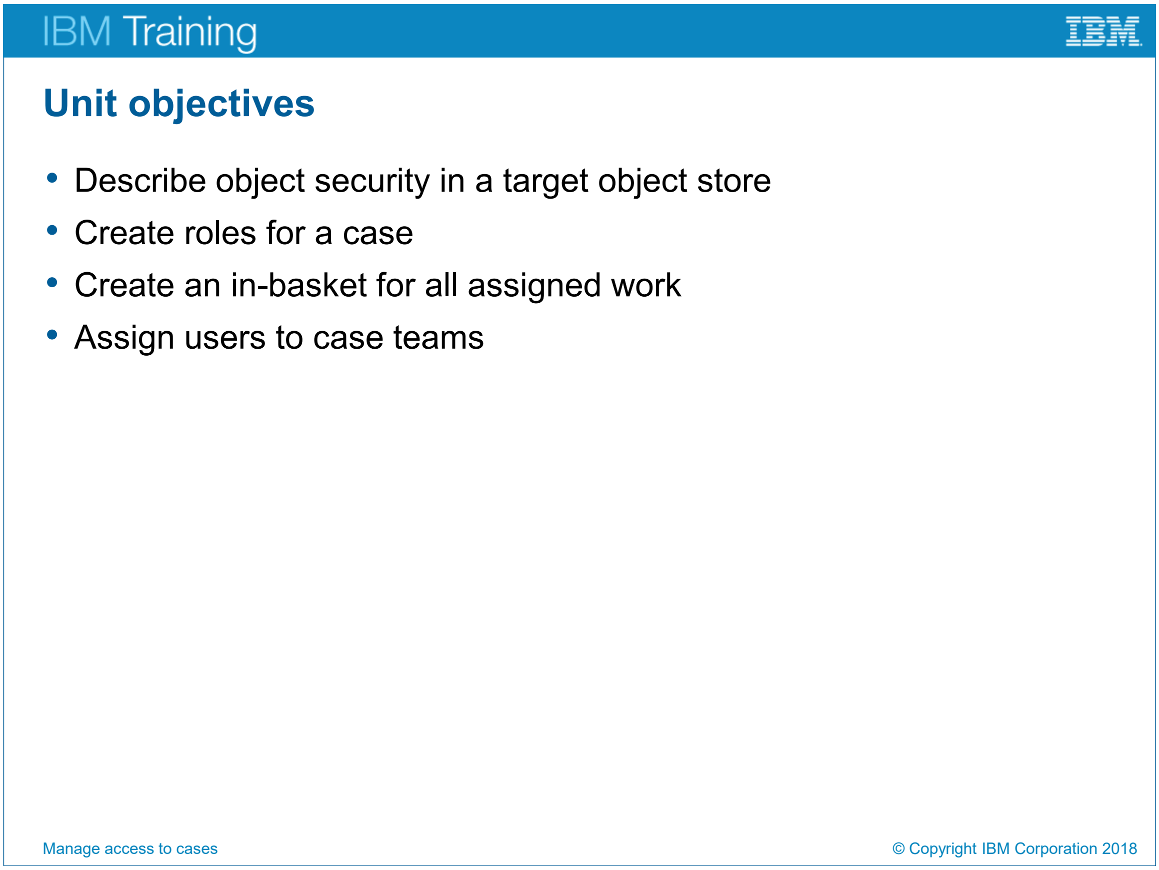
Unit 3 Manage access to cases



IBM Training

Manage access to cases

IBM Case Manager V5.3.2



IBM Training

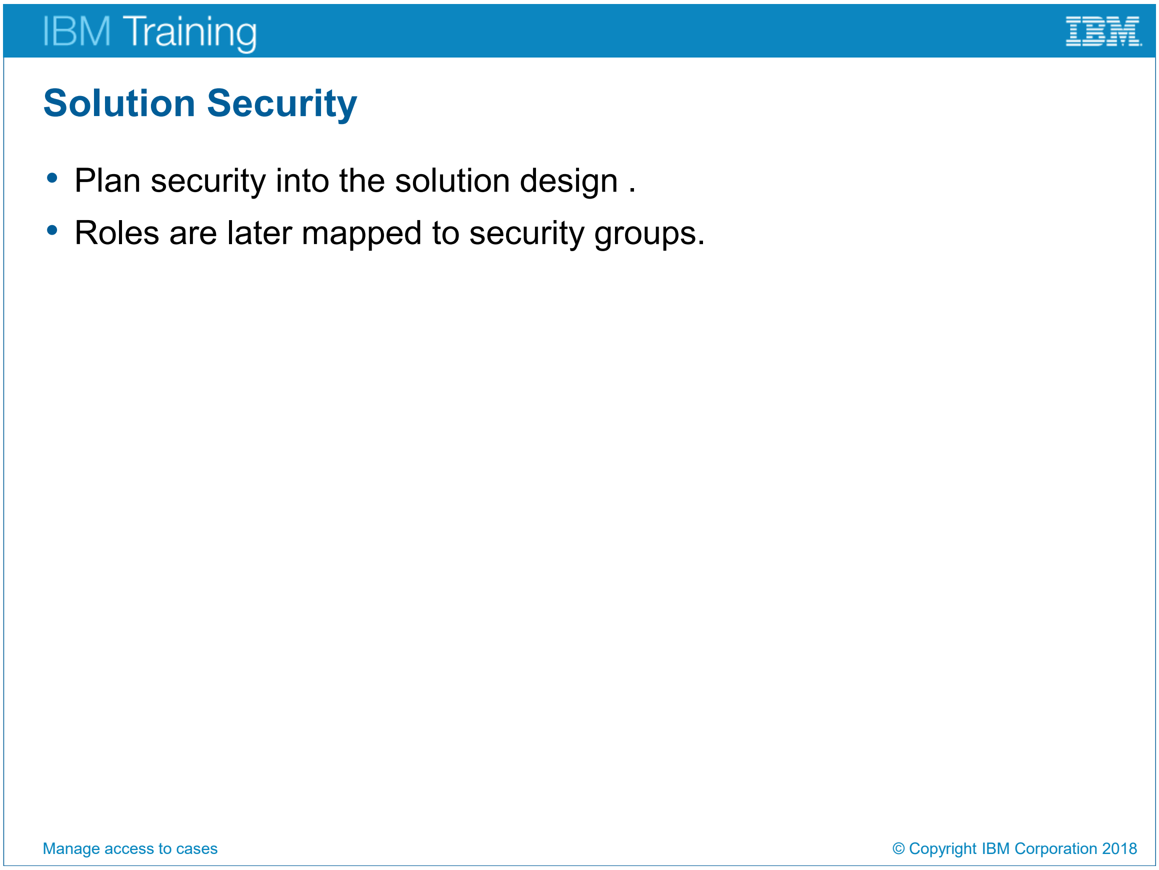
Unit objectives

- Describe object security in a target object store
- Create roles for a case
- Create an in-basket for all assigned work
- Assign users to case teams

Manage access to cases

© Copyright IBM Corporation 2018

Unit objectives



IBM Training

Solution Security

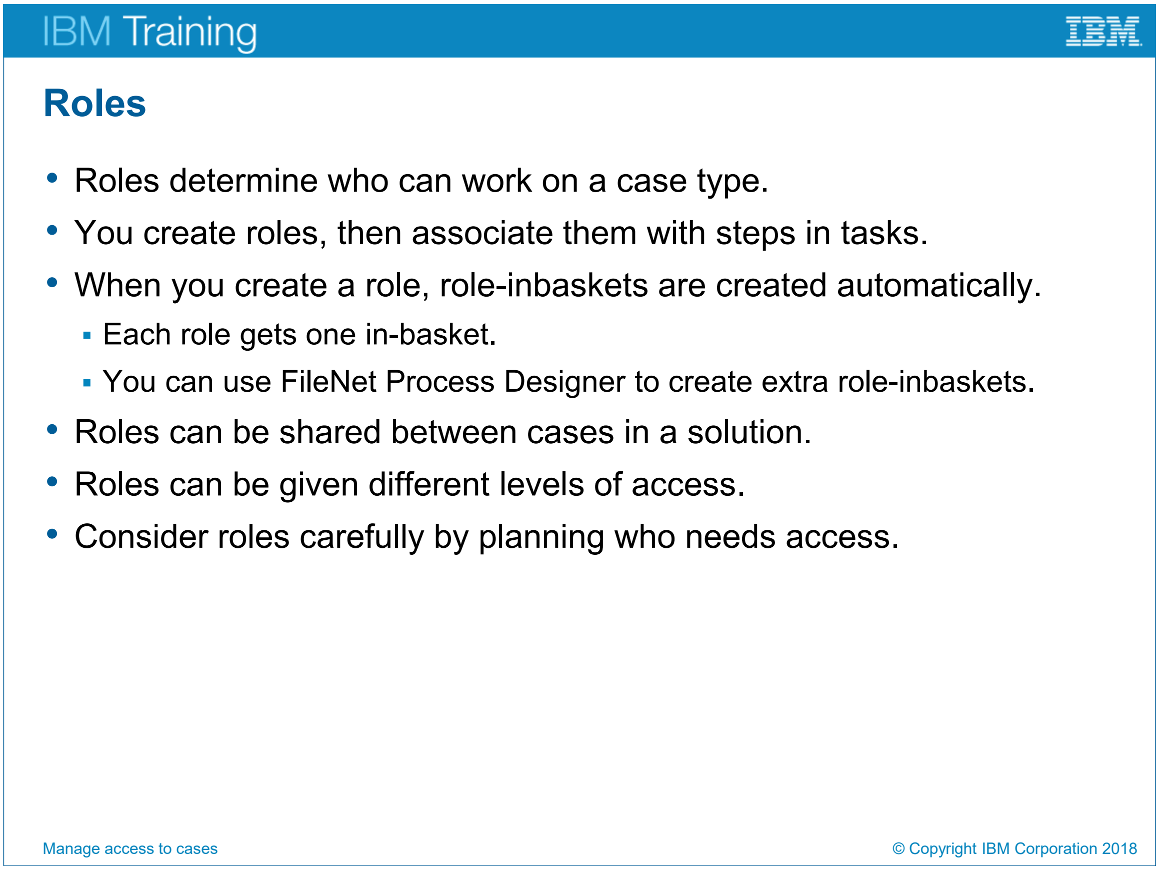
- Plan security into the solution design .
- Roles are later mapped to security groups.

Manage access to cases

© Copyright IBM Corporation 2018

Solution Security

The solution architect must plan security for the solution as part of the initial solution design. As a solution architect, you must create roles for the solution that can later be mapped to security groups.



IBM Training

Roles

- Roles determine who can work on a case type.
- You create roles, then associate them with steps in tasks.
- When you create a role, role-inbaskets are created automatically.
  - Each role gets one in-basket.
  - You can use FileNet Process Designer to create extra role-inbaskets.
- Roles can be shared between cases in a solution.
- Roles can be given different levels of access.
- Consider roles carefully by planning who needs access.

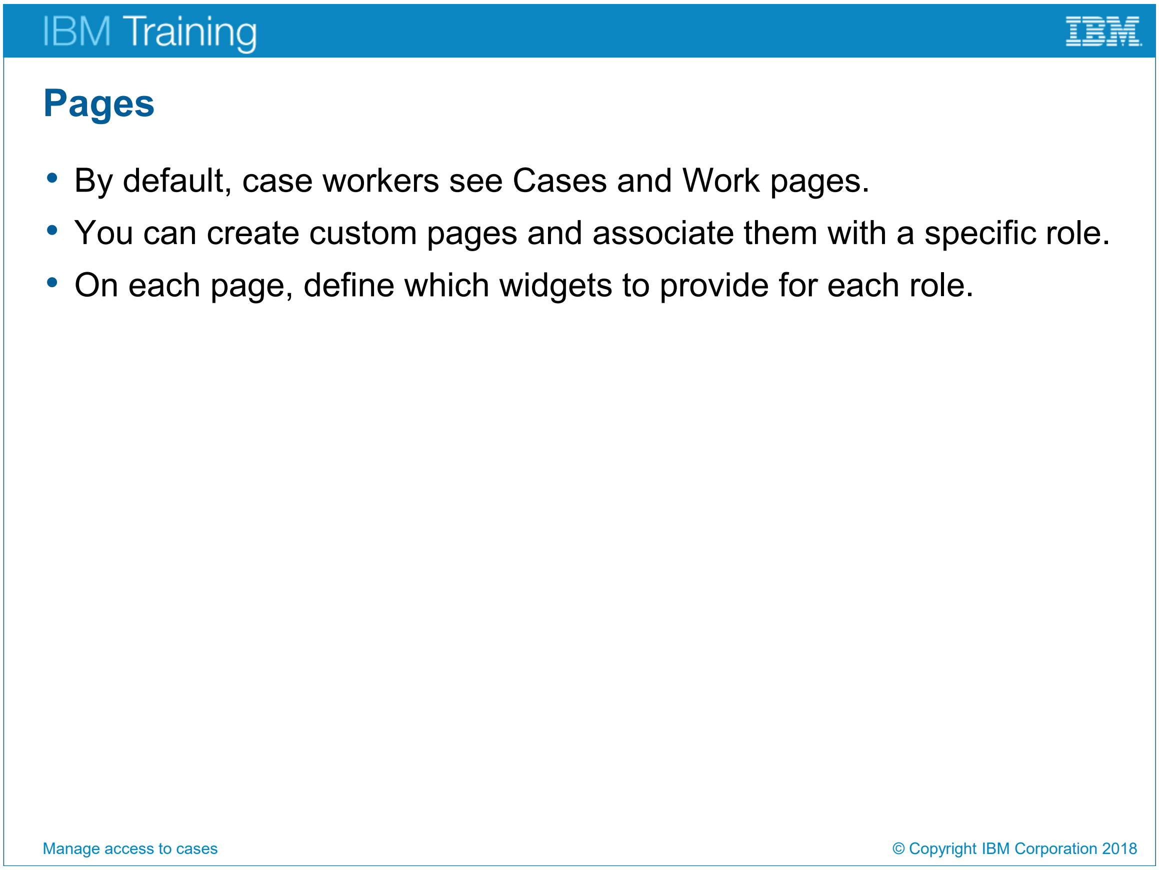
Manage access to cases

Roles

Roles determine who can work on each case type. Roles can be given different levels of access. When you plan security for roles, consider the following questions:

- Who needs access to the case?
- Who can view case information?
- Who can update case information?
- Who can start new cases?
- Who can start new tasks?
- Can users start discretionary tasks?
- Who can add documents to a case?
- Who can add comments to a case?
- Can supervisors see other in-baskets or assigned work?

Assigning a user to a role does not provide that user object store permissions. For full access to cases and case artifacts, users must also have sufficient object store rights.



IBM Training

Pages

- By default, case workers see Cases and Work pages.
- You can create custom pages and associate them with a specific role.
- On each page, define which widgets to provide for each role.

Manage access to cases

© Copyright IBM Corporation 2018

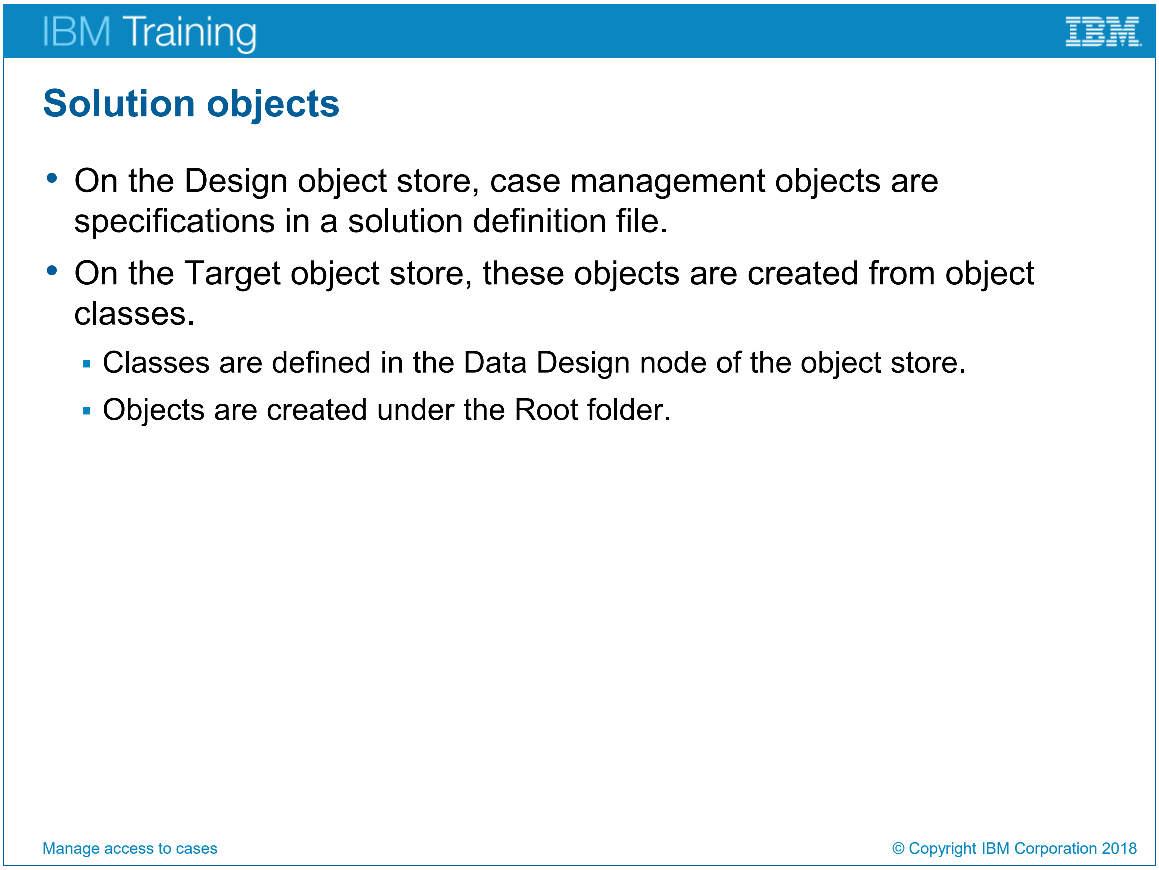
Pages

In Case Manager Builder, you specify Pages for each role on the Pages tab of the role.

Solution pages provide case workers with access to cases and work items that are in a solution. By default, the two IBM Case Manager Solution pages, Cases and Work, are used for every role.

The Solution pages are displayed when a user first opens the solution in Case Manager Client. These pages remain open during the user's session.

You can create custom Solution pages to meet the needs of a specific role. You then associate the custom pages with that role.



IBM Training

Solution objects

- On the Design object store, case management objects are specifications in a solution definition file.
- On the Target object store, these objects are created from object classes.
  - Classes are defined in the Data Design node of the object store.
  - Objects are created under the Root folder.

Manage access to cases

© Copyright IBM Corporation 2018

Solution objects

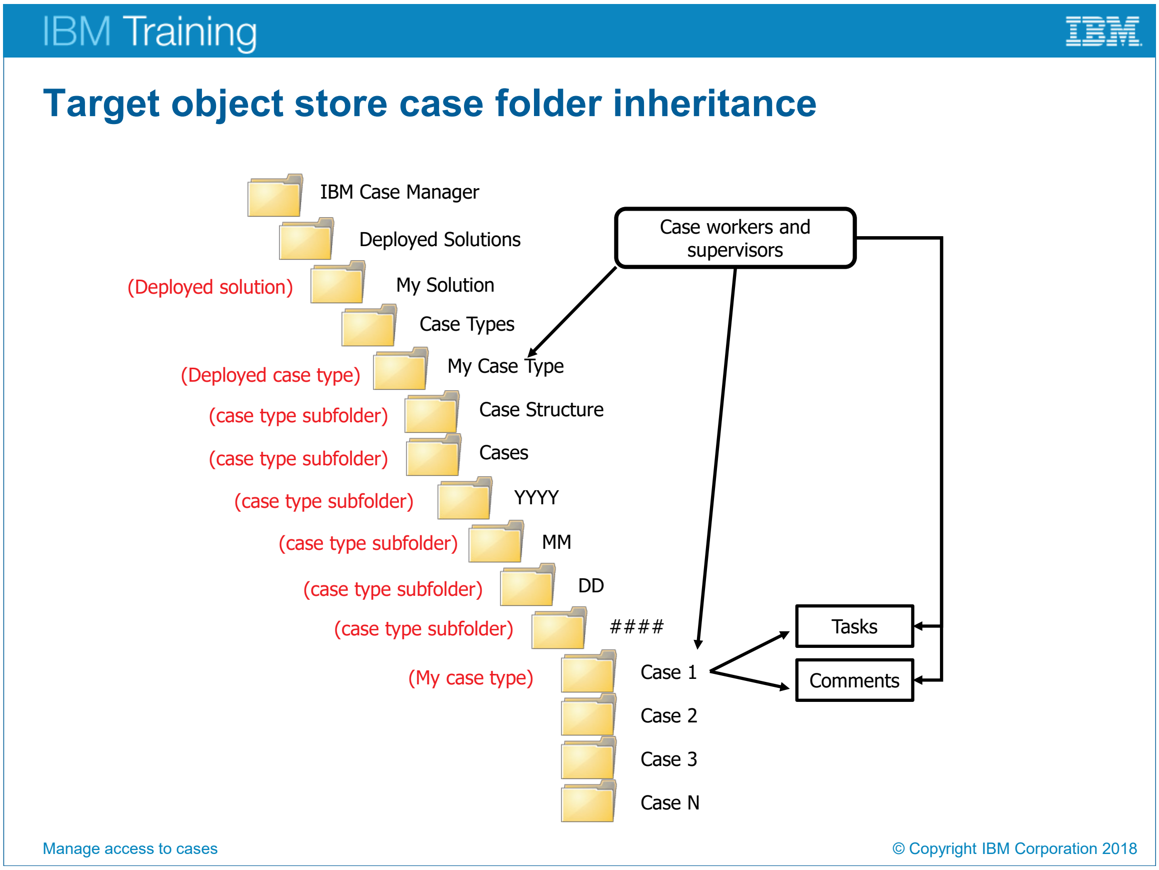
Solution objects include:

- Case folders
- Case properties
- Document classes

The solution objects exist only as specifications in a solution definition file. They are not separate objects that can be secured with access control lists.

On the target object store, solution objects are created when the solution is deployed. A number of factors determine solution object security, including:

- Object store security.
- Inheritance specifications.
- Default instance security on the class definition.



IBM Training

Target object store case folder inheritance

IBM Case Manager

Deployed Solutions

(Deployed solution) My Solution

Case Types

(Deployed case type) My Case Type

(case type subfolder) Case Structure

(case type subfolder) Cases

(case type subfolder) YYYY

(case type subfolder) MM

(case type subfolder) DD

(case type subfolder) ####

(My case type) Case 1

Case 2

Case 3

Case N

Case workers and supervisors

Tasks

Comments

Manage access to cases

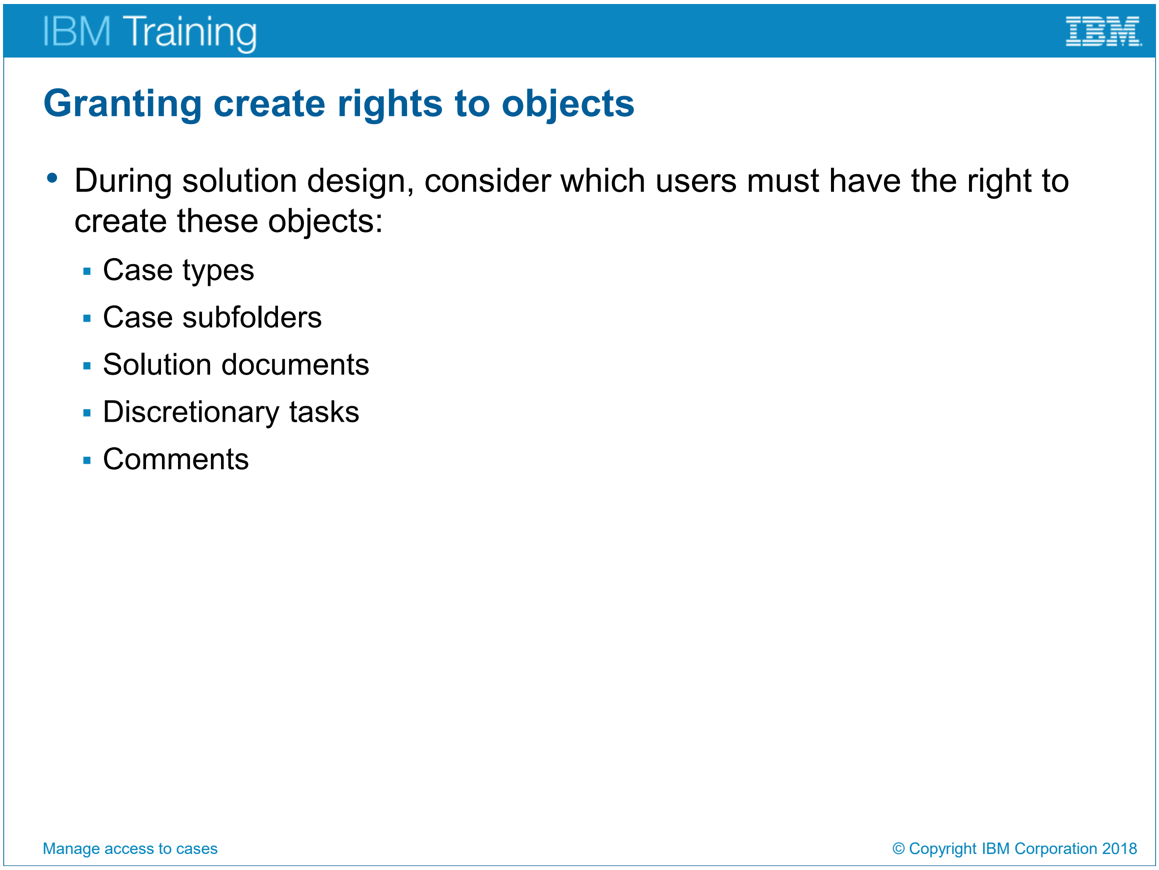
© Copyright IBM Corporation 2018

Target object store case folder inheritance

The graphic shows how security is inherited down from the case type folder to the individual case objects. In a target object store, case object security is inherited from the case folder, which inherits security from the case type folder. Unless you use default instance security or other security specifications, the inheritance model provides security for the case artifacts.

Security is configured on the deployed case type folder on the target object store.

All case instances are contained in this case type folder, from which they inherit security settings.



IBM Training

Granting create rights to objects

- During solution design, consider which users must have the right to create these objects:
  - Case types
  - Case subfolders
  - Solution documents
  - Discretionary tasks
  - Comments

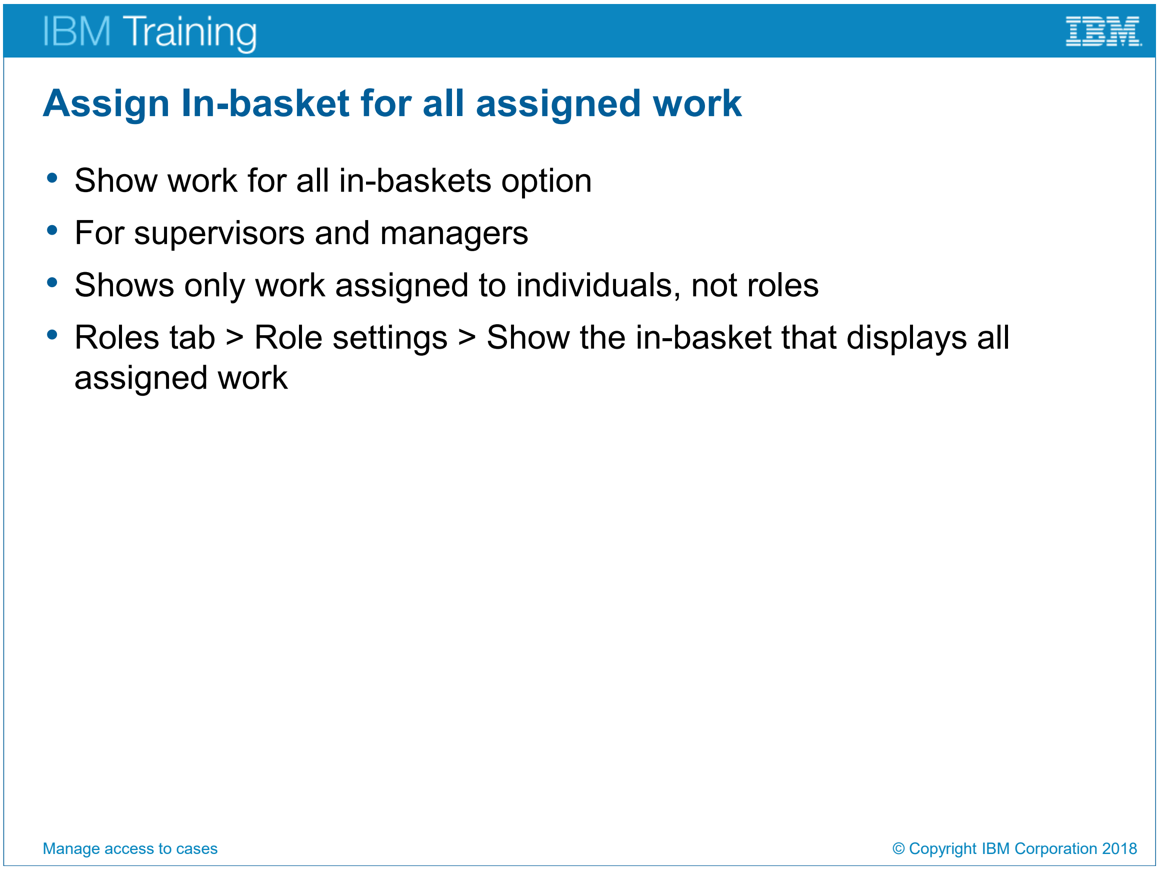
Manage access to cases

Granting create rights to objects

Security is most efficiently handled through roles and security configurations. Sometimes, however, you might need to specify security settings on classes.

You must consider which users must have the right to create these objects:

- Case types are subclasses of the Case Folder class. On the target object store, the Deployed Case Type folder needs to be secured.
- Case Subfolder uses the default folder class. However, a user must have permission to create subfolders in a case folder or subfolder.
- Solution document types are subclasses of the Document class. Users also need File in Folder rights on the case folder to create documents in a case.
- Discretionary task types, Quick tasks, and To Do tasks are subclasses of Case Task. Users also need Process Services Roster create right.
- Comments are annotations on the case folder. Users must have Annotate rights on the case folder. Case Types are subclasses of the Case Folder class.



IBM Training

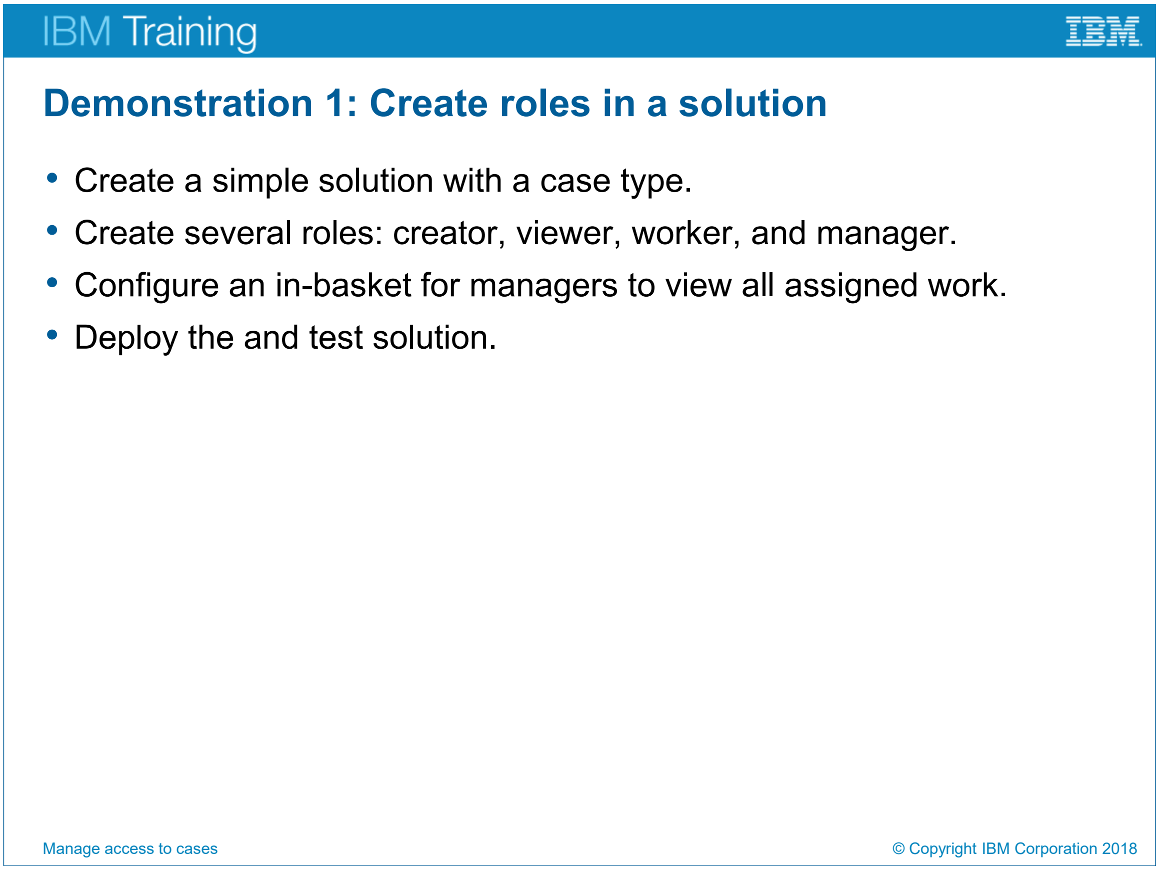
Assign In-basket for all assigned work

- Show work for all in-baskets option
- For supervisors and managers
- Shows only work assigned to individuals, not roles
- Roles tab > Role settings > Show the in-basket that displays all assigned work

Manage access to cases

Assign In-basket for all assigned work

When you are creating roles, you can optionally allow a role to have an in-basket that shows all assigned work. This in-basket is useful for supervisors who need to have an overview of work assignments. The all assigned work in-basket displays a list of all the open work items that are assigned to users. Work items that are assigned to roles are not listed.



IBM Training

Demonstration 1: Create roles in a solution

- Create a simple solution with a case type.
- Create several roles: creator, viewer, worker, and manager.
- Configure an in-basket for managers to view all assigned work.
- Deploy the and test solution.

Manage access to cases

© Copyright IBM Corporation 2018

Demonstration 1: Create roles in a solution

Demonstration 1: Create roles in a solution

Purpose:
You are going to be developing a solution for a medical company. The solution design is simple to start with, but you need to ensure that the roles are properly configured. The first case type is for patients who walk in without an appointment.

Case Manager Builder URL: **http://vclassbase:9081/CaseBuilder**

Solution builder Username: **Paula**

Solution builder Password: **FileNet1**

Task 1. Create a solution.

1. Use **Firefox** to log in to **Case Manager Builder** as **Paula/FileNet1**.
2. Create a solution.
   - **Solution name**: `Medical Visit`
   - **Solution Prefix**: `MED`
3. On the **Properties** page, add a **String** property named `Client Name`.

Task 2. Add roles.

In this task, you add roles to the solution. The Physician role includes the responsibility of monitoring the in-baskets of the other roles.

1. Open the **Roles** tab.
2. Click **Add Role**.
3. Type `Insurance Coordinator` into the **Role** field, then click **OK**.
4. Verify that the following options are selected:
   - **Personal (Common): Show the common view**.
   - **Role members can move work into their personal in-basket**.
   - **Role members can reassign work to others**.
5. Add the **Nurse** role with the same options.
6. Add the **Receptionist** role with the same options.

7. Add the **Physician** role with the following options:
    - **Personal (Role): Show a custom view for this role**.
    - **Role members can move work into their personal in-basket**.
    - **Role members can reassign work to others**.
    - **Show the in-basket that displays all assigned work**.
8. Click **OK All**.
9. Click **Save**.

Task 3. Add a case type.

1. Open the **Case Types** tab.
2. Click **Add Case Type**.
3. Case type name: `Office Visit`.
4. On the **Properties** tab, add the **Client Name** property, then click **Save**.
5. On the **Views** tab, add the following properties to **Case Summary** view:
    - **Client Name**
    - **Added On**
    - **Added by**
6. On the **Case Folders** tab, add the following case folders, then click **Save**:
    - **Medical records**
    - **Insurance documents**
    - **Notes**
7. On the **Tasks** tab, click **Add Task** > **Task**.
8. Name: `Initial Consultation`, then click **OK**.
9. Save the solution.

Task 4. Add role lanes.

1. Hover the mouse cursor over the task.
2. Click **Edit Steps** .
3. Drag a role lane into the working area.
4. Select the **Receptionist** role.
5. Add the **Insurance Coordinator** role lane.

6. Add the **Nurse** role lane.

   You might need to reduce the browser zoom setting to see the space at the bottom of the role lanes.

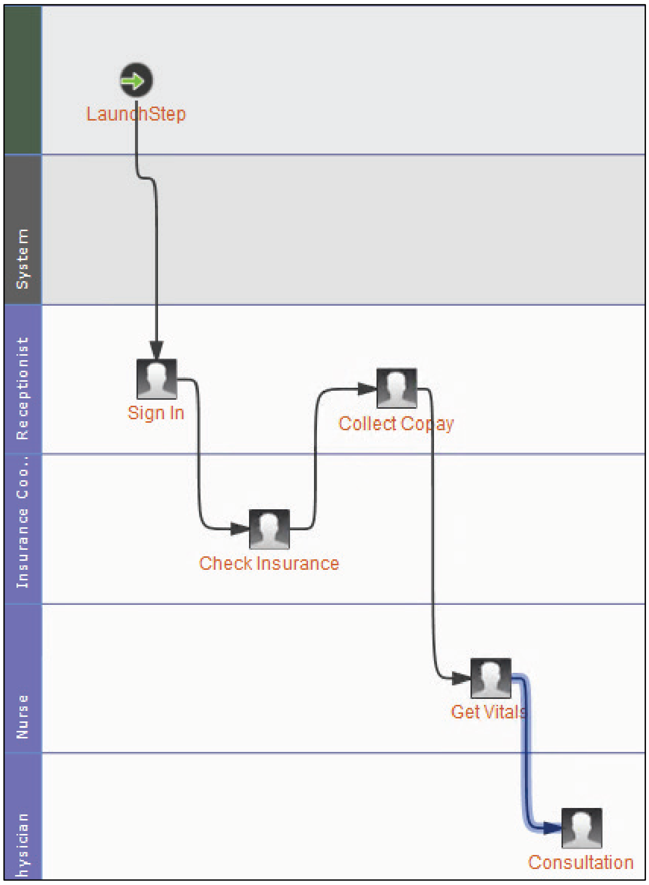
7. Add the **Physician** role lane.

Task 5. Add steps to the task.

In this task you add steps to the role lanes and then connect them. The Receptionist has two steps. The other roles each have one step.

1. Drag a step into the **Receptionist** role lane and name the step **`Sign In`**.
2. Drag a step to the **Insurance Coordinator** role lane named **`Check Insurance.`**
3. Drag a step to the **Receptionist** role lane named **`Collect Copay.`**
4. Drag a step to the **Nurse** role lane named **`Get Vitals.`**
5. Drag a step to the **Physician** role lane named **`Consultation`**.
6. Click the **Add Connections between steps** button ⤡.
7. Connect the **Launch** step to the **Sign In** step. Connect the rest of the steps in the order given in Task 5.

   The results appear as follows:

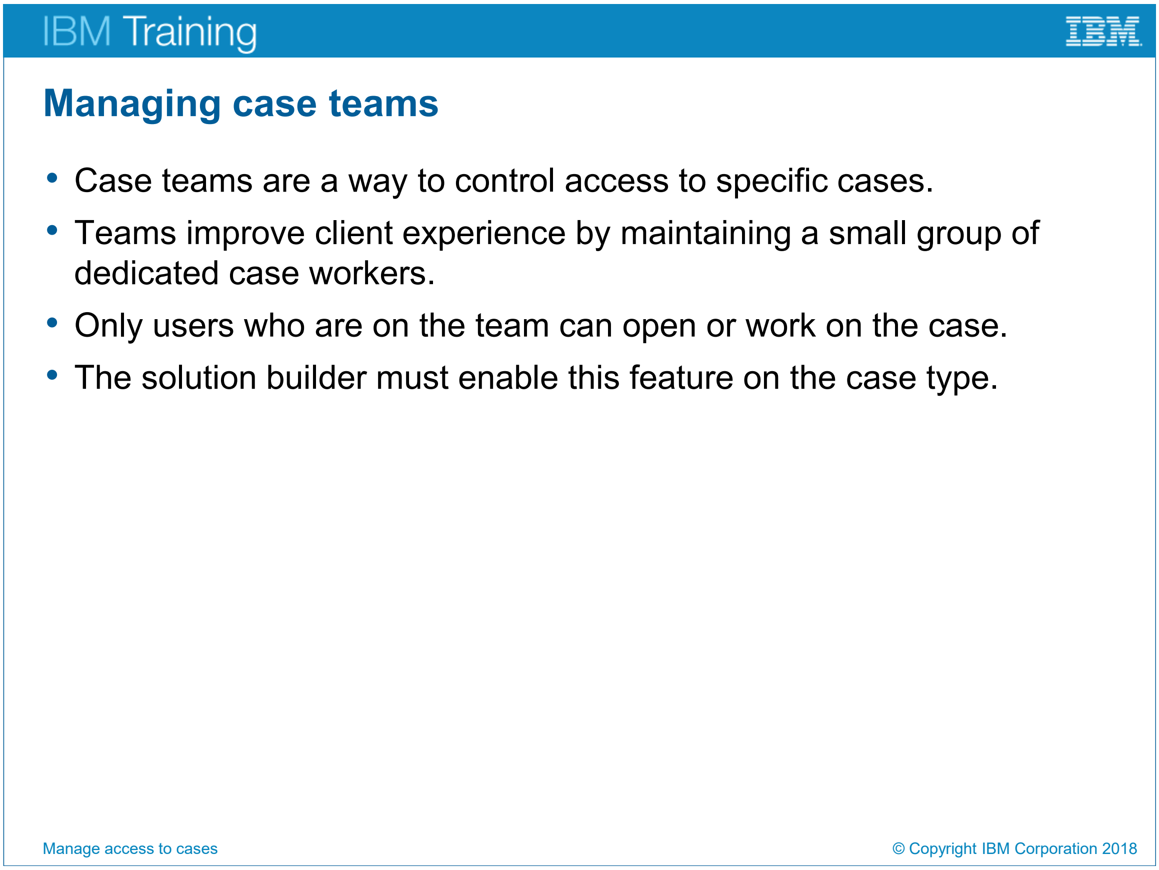


8. Add the **Client Name** property to the **Sign In** step by completing the following steps:
   - Select the **Sign In** step.
   - Click the ellipsis button ... next to **Properties**.
   - Click **Select Properties** > **Select All** > **OK** > **OK**.
9. Open each remaining step and add the **Client Name** property.
10. **Save**, **Validate** ✓, and then **Close** the task.
11. Click **Validate**, then **Save and Close** the solution.

Task 6. Deploy the solution.

1. On the Manage Solutions page, deploy ↻ the Medical Visit solution.
2. Wait for the deployment to complete.
3. Log out of all applications and close all browsers.

Result:
You created a solution with four roles. The solution includes a task. Users who are assigned to these roles can open cases and complete tasks. You use this solution for later demonstrations.



IBM Training

Managing case teams

- Case teams are a way to control access to specific cases.
- Teams improve client experience by maintaining a small group of dedicated case workers.
- Only users who are on the team can open or work on the case.
- The solution builder must enable this feature on the case type.

Manage access to cases

© Copyright IBM Corporation 2018

Managing case teams

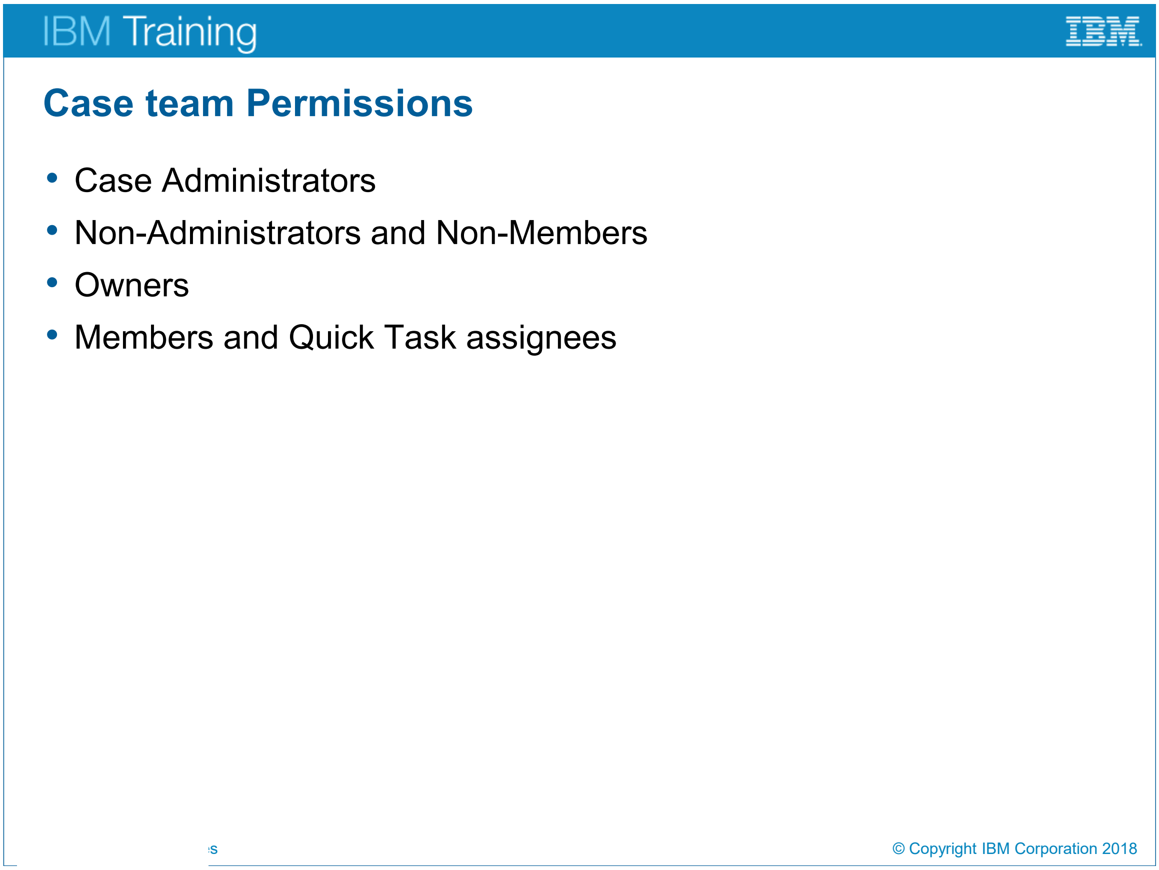
With case teams, case workers can control which case workers have access to a case. This feature is useful if your organization has many case workers in a role, but you want the case to be handled by a small group of workers who become familiar with the case. This personal touch can greatly improve the client experience.

Without teams, when a case opens, all case workers in a given role have access to a case. This type of case assignment is good for high-volume case types. For example, when a new troubleshooting ticket opens, any one of three hundred level 1 ticket handlers might work on the case. When the task is completed, the case might go back to the role inbox to be handled by another ticket handler.

For some applications, you might want to restrict the number of people involved in the case. For example, in a healthcare-related case type, you want to have a small team of nurses and doctors working on a case to ensure that the case workers are all familiar with the case history.

The case owner can assign team members to the case. From that point, only team members have access to the case. By default, the person who starts a case is the case owner.

As a solution builder, you need to decide whether to allow case owners to manage teams.



IBM Training

Case team Permissions

- Case Administrators
- Non-Administrators and Non-Members
- Owners
- Members and Quick Task assignees

s

Case team Permissions

IBM Case Manager administrators can access a Work Item in read-only mode, even if there is a Case Team assigned to the case.

If a work item or a case has been assigned a case team, then users who are not members of the case team cannot open the work item or the case details page. A notice alerts these users that they are not part of the assigned team and so access is restricted.

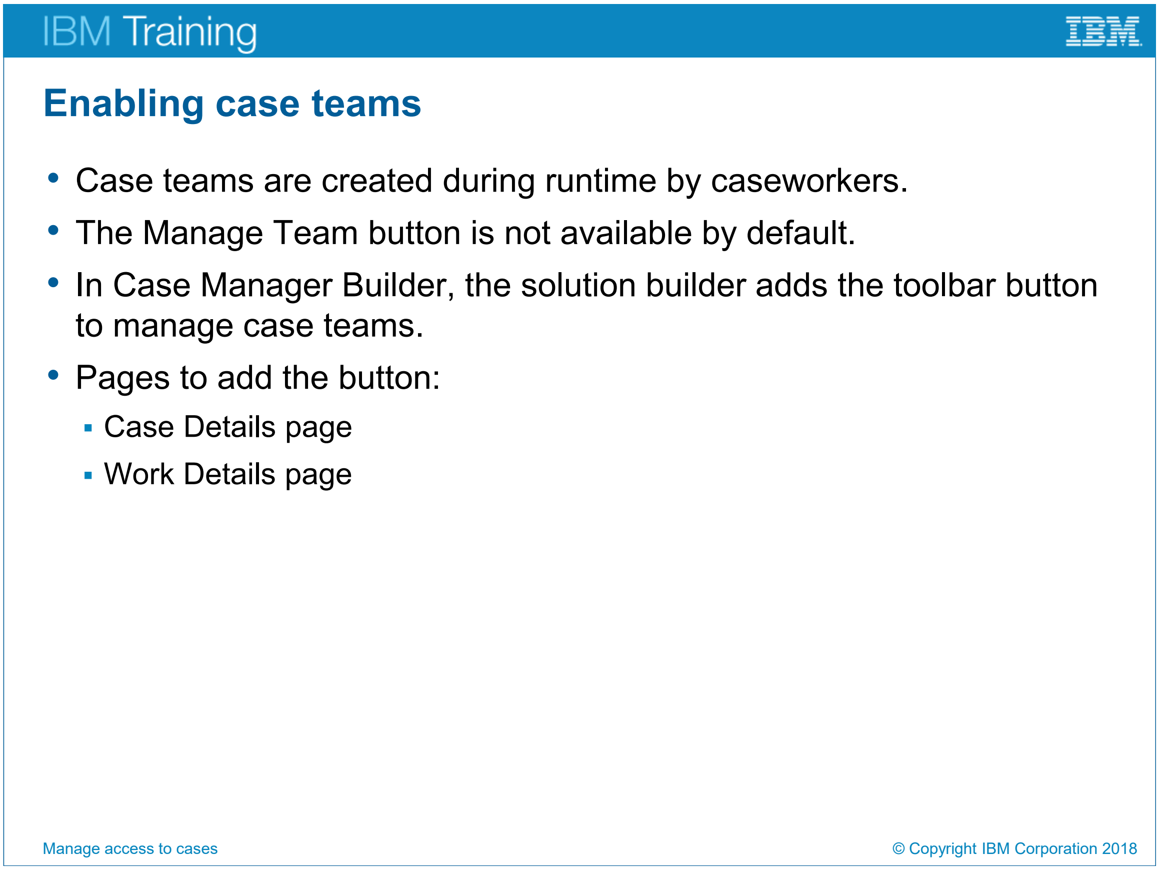
Cases without team membership function as before. Any user who has access to the Solution/Role can view the case.

Case owners:

- Can add and remove Members
- Can add and remove other Owners
- Cannot remove themselves

Team members and quick-task assignees:

- Can access and view the case
- Can view case team members
- Cannot modify case team members



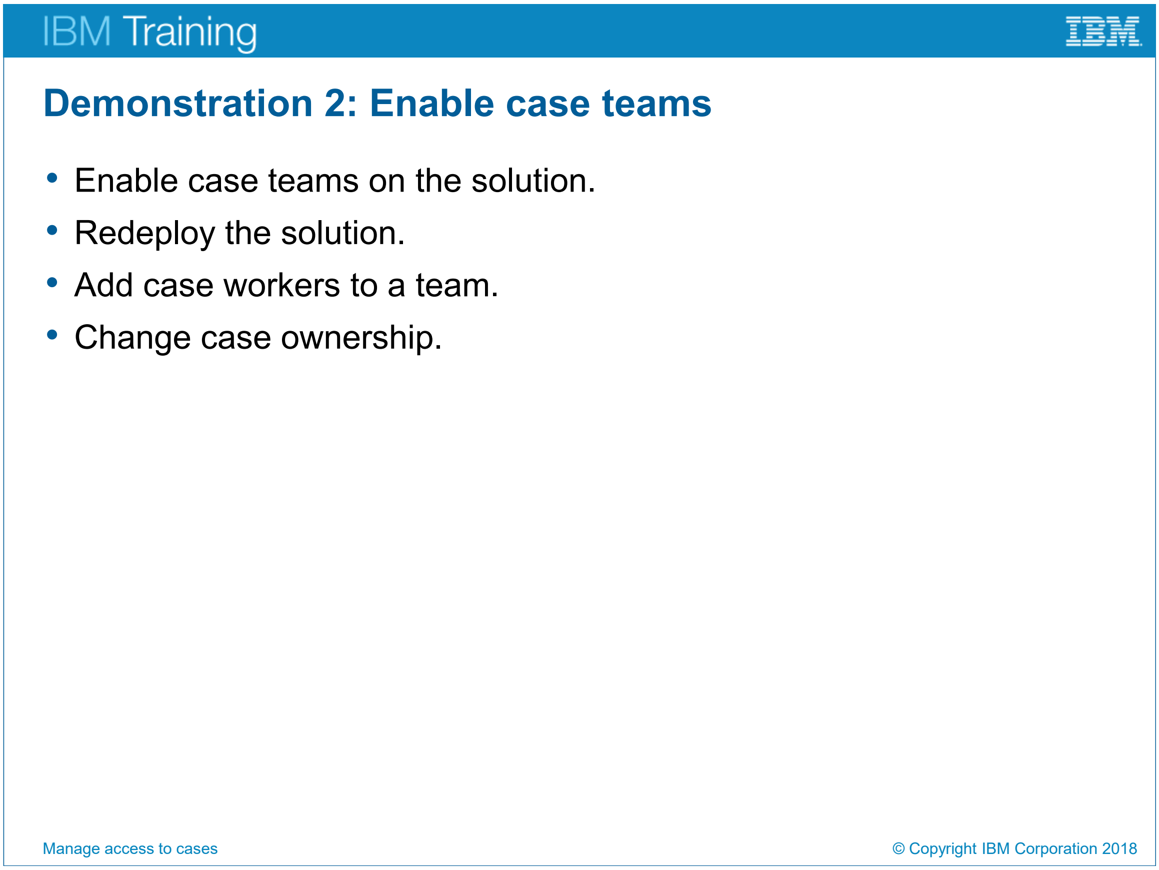
IBM Training

Enabling case teams

- Case teams are created during runtime by caseworkers.
- The Manage Team button is not available by default.
- In Case Manager Builder, the solution builder adds the toolbar button to manage case teams.
- Pages to add the button:
  - Case Details page
  - Work Details page

Manage access to cases

Enabling case teams



IBM Training

Demonstration 2: Enable case teams

- Enable case teams on the solution.
- Redeploy the solution.
- Add case workers to a team.
- Change case ownership.

Manage access to cases

Demonstration 2: Enable case teams

Demonstration 2: Enable case teams

Purpose:
In this solution, clients expect personalized care from their health-care providers. You are going to enable and test the case team feature so that each case can have a small, dedicated team of caseworkers.

Case Manager Builder URL: **http://vclassbase:9081/CaseBuilder**

Case Manager Client URL: **http://vclassbase:9081/navigator/?desktop=icm**

Solution builder Username: **Paula**

Solution builder Password: **FileNet1**

Task 1. Copy the Medical Visit solution

In this task you create a copy of the Medical Visit solution so that you can manage case teams without affecting the original solution, which is used in later demonstrations.

1. Use **Firefox** to log into **Case Manager Builder** as **Paula/FileNet1**.
2. Click the **Actions** button ⋮ and select **Copy**.
3. Enter the following information and then click **OK**.
   - **Name**: `Team Test`
   - **Solution prefix**: `TEAM`

Task 2. Edit the Case Details page.

In this task you add the Manage Team button to the Case Details page so that caseworkers can manage teams.

1. Open the **Team Test** solution for editing.
2. Open the **Pages** tab.
3. Expand the **Case Details** node and then click **Case Details** to edit the **Case Details** page.
4. Click **Edit Settings** ⚙ to edit the settings for the **Case Toolbar** widget.
5. Click the **Toolbar** tab.
6. Click **Add Button** ▭.
7. From the **Action** menu, select **Manage Team**, then click **OK**.
8. Click **OK** to close the **Case Toolbar** widget settings.

9. Save the page, then close **Page Designer**.
10. Save and close the solution.

Task 3. Deploy the solution.

1. Deploy the solution.
2. Click **Test** ▶ to test the solution in **Case Manager Client**.

   Optionally, you can open Case Manager Client by using the Case Client link on the Home page.

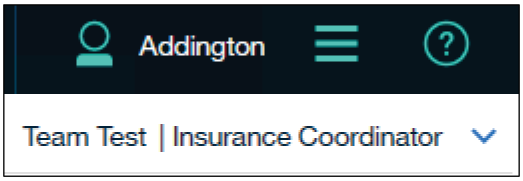
Task 4. Manage roles.

1. Click **Team Test** > **Manage Roles**.
2. For each role, select the role, then click **Add Users and Groups**, then search for and add the user:
   - **Insurance coordinator**: **Paula**, **Addington**
   - **Nurse**: **Paula**, **Sue**
   - **Receptionist**: **Paula**, **Cody**
   - **Physician**: **Paula**, **Fred**
3. Click **Save**, then log out of **Case Manager Client**.
4. Close **Firefox**.

Task 5. Test user access.

1. Open **Firefox**, then click the **Case Client** link from the Home page.
2. Log in to **Case Manager Client** as **Addington/FileNet1**.
3. Click the **Cases** tab.
4. Verify the settings:
   - Solution: **Team Test**
   - Role: **Insurance Coordinator**.

   The results appear as follows:



Addington

Team Test | Insurance Coordinator

5. Log out.

6. Log in to **Case Manager Client** and then select the **Team Test** solution > *role* to verify that each account belongs to the correct role, then log out:
   - **Sue: Nurse**
   - **Fred: Physician**
   - **Cody: Receptionist**

Task 6. Create a case

1. Log in to **Case Manager Client** as **Paula/FileNet1**.
2. Verify that you are in the **Team Test** solution.
3. Click **Add Case** > **Office Visit**.
4. In the **Client Name** field type `Client1,` then click **Add**.
5. Log out of **Case Manager Client**.

Task 7. View the case without a team.

1. Log on to **Case Manager Client** as **Cody/FileNet1**.
2. Click **Search** to find the case.
3. Click the case to open it in the **Case Details** page.
4. Click the **Work** tab.
5. Verify that you can see a work item: **Sign In**.
6. Open the work item to verify that you can open it.
7. Close the work item.
8. Log out of **Case Manager Client**.

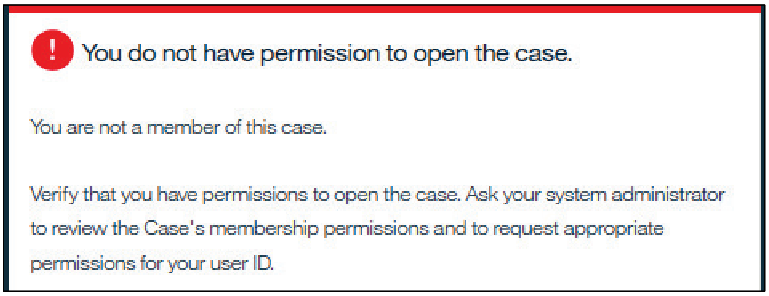
Task 8. Create a case team.

1. Log in to **Case Manager Client** as **Paula/FileNet1**.
2. Search for your case, then open it.
3. Click **Manage Team**.
4. With the **Insurance Coordinator** role selected, verify that you can see **Addington** and **Paula** in the **Available** area.
5. Select **Paula**, then click the **Add** arrow.
6. Click the **Nurse** role.
7. Add **Paula** to the **Nurse** role.
8. Add **Paula** to the **Receptionist** role.
9. Add **Paula** to the **Physician** role.
10. Click **Save**.
11. Click **Close**, then log out of **Case Manager Client**.

Task 9. View the case team effects.

1. Log in to **Case Manager Client** as **Cody/FileNet1**.
2. Search for the case, then attempt to open it.

   You receive a message that indicates that you do not have permission to view the case.



! You do not have permission to open the case.

You are not a member of this case.

Verify that you have permissions to open the case. Ask your system administrator to review the Case's membership permissions and to request appropriate permissions for your user ID.

3. Close the permission message.
4. Click the **Work** tab.
5. Attempt to open the work item. Confirm that you are not permitted.
6. Log out of **Case Manager Client**.

Task 10. Add a team owner.

Case owners can add and remove case team members.

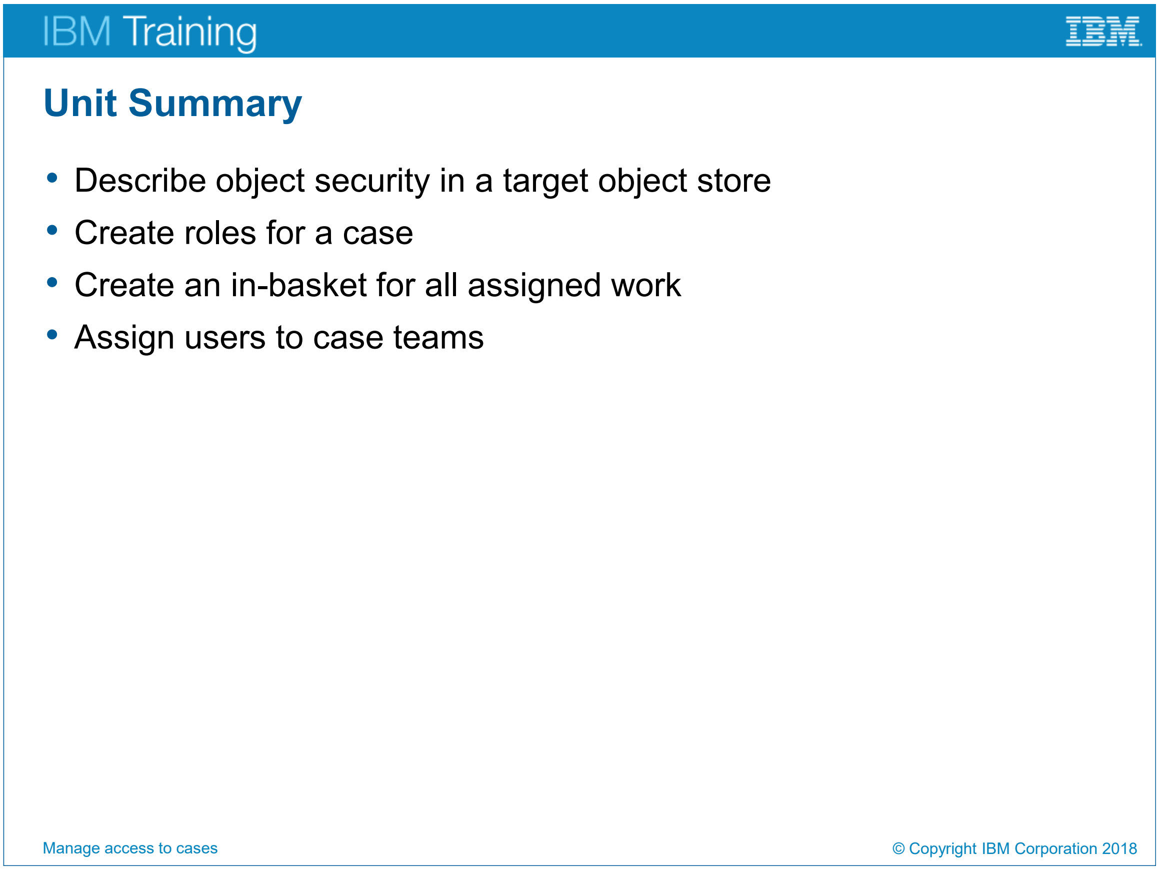
1. Log in to **Case Manager Client** as **Paula/FileNet1**.
2. Search for your case, then open it.
3. Click **Manage Team**.
4. Click the **Physician** role.
5. Add **Fred** to the **Case Team**.
6. Select **Fred**, then click **Make Owners.**
7. Click **Save**.
8. Log out of **Case Manager Client**.

Task 11. Remove Team Test solution.

Remove this solution to avoid confusion in future demonstrations.

1. Use **Firefox** to log into **Case Manager Builder** as **Paula/FileNet1**.
2. On the **Solutions** page, on the **Team Test** solution, click **Actions** > **Remove**.
3. Confirm that only the **Medical Solution** is shown on the **Solutions** page.
4. Log out of all applications and close all browsers.

Result:
You enabled case team management in the solution, then created a case team and viewed the effects. You also added a case owner.



IBM Training

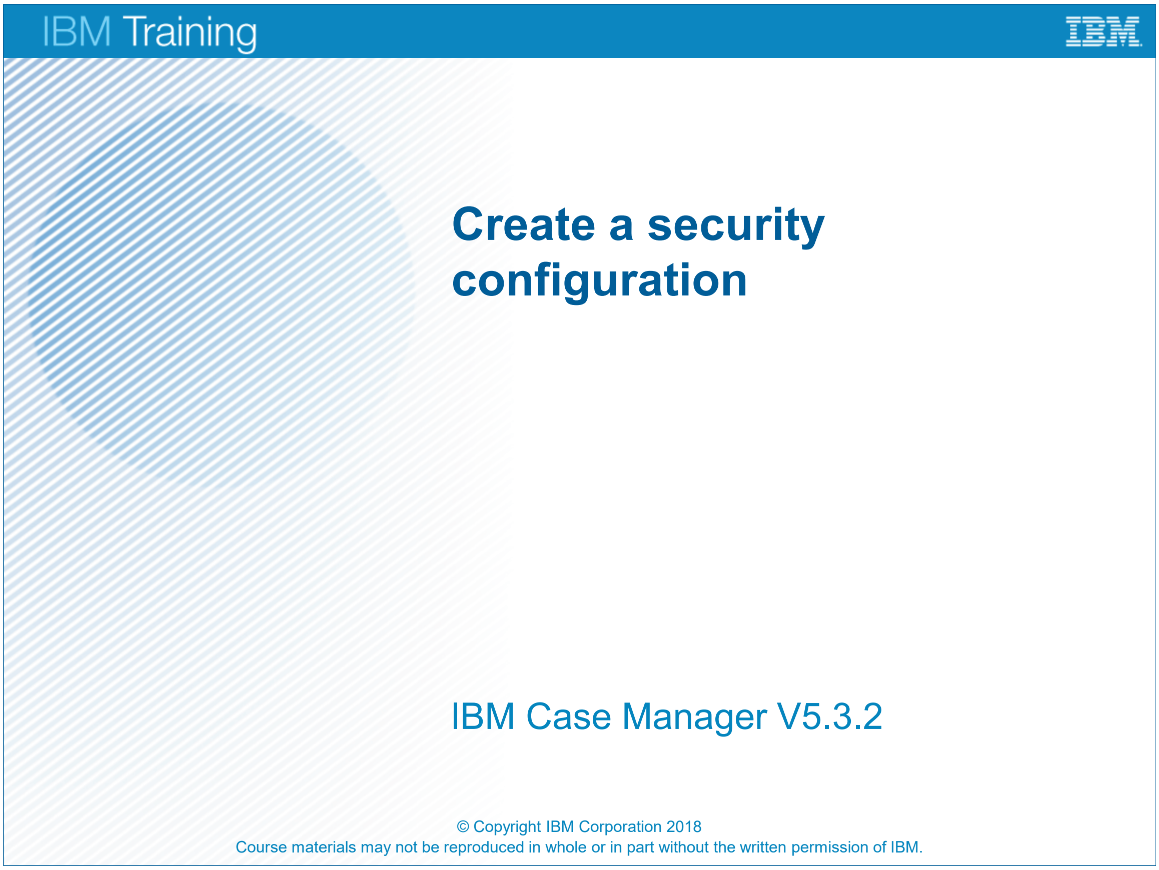
Unit Summary

- Describe object security in a target object store
- Create roles for a case
- Create an in-basket for all assigned work
- Assign users to case teams

Manage access to cases

Unit Summary

Unit 4 Create a security configuration

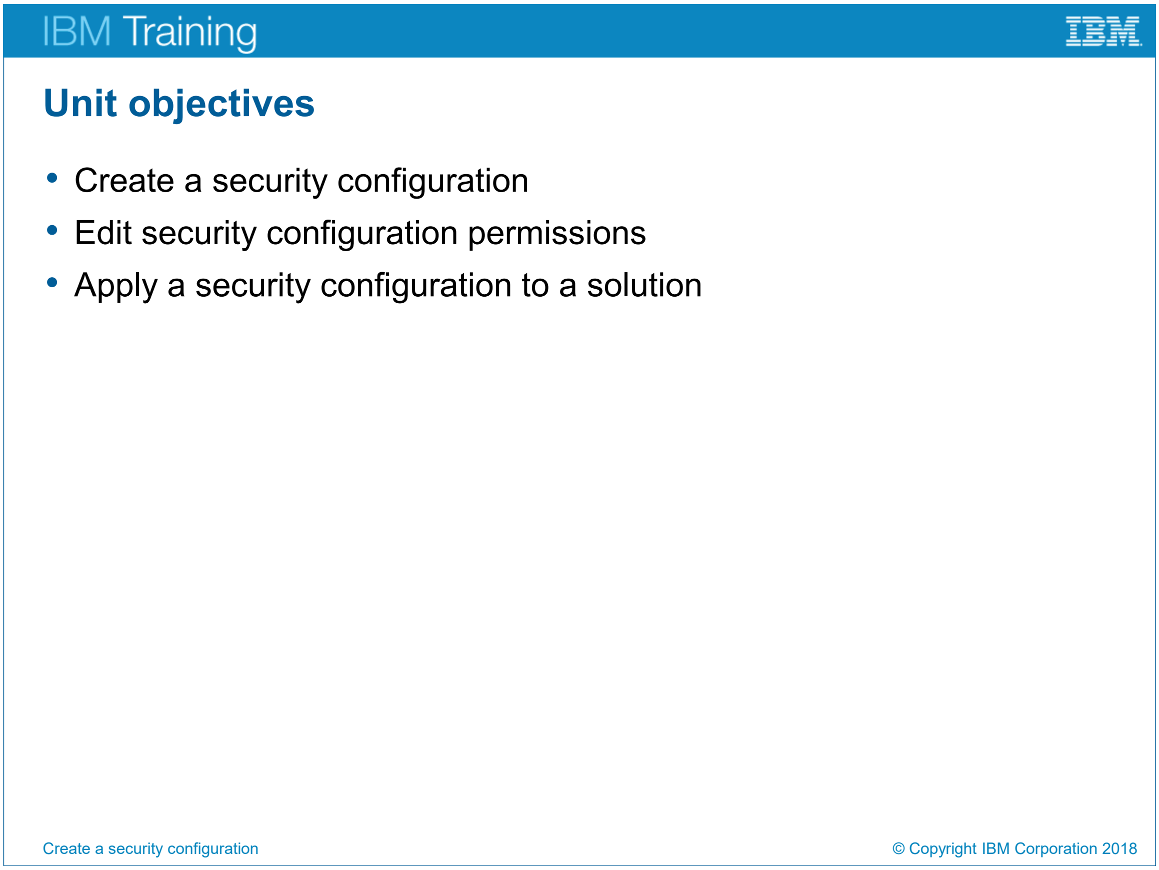


IBM Training

IBM

Create a security configuration

IBM Case Manager V5.3.2



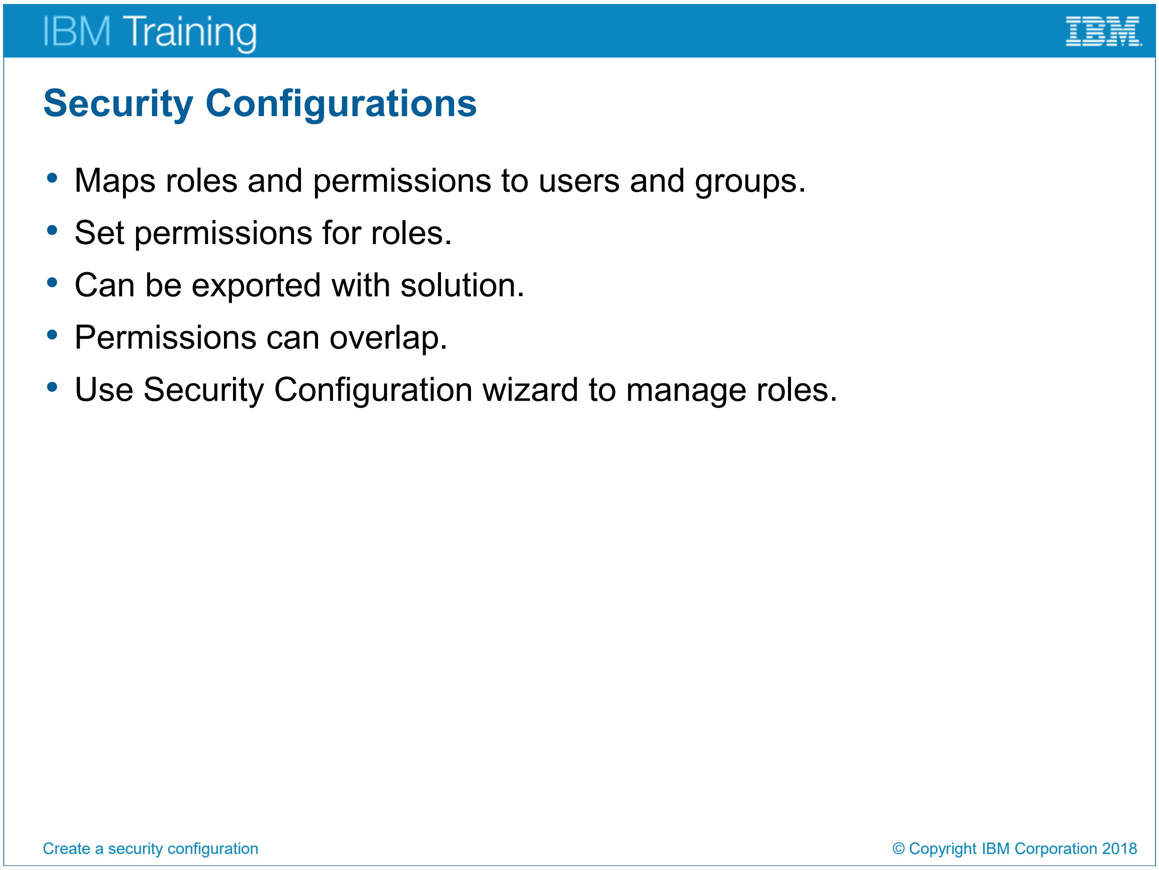
IBM Training

Unit objectives

- Create a security configuration
- Edit security configuration permissions
- Apply a security configuration to a solution

Create a security configuration

Unit objectives



IBM Training

Security Configurations

- Maps roles and permissions to users and groups.
- Set permissions for roles.
- Can be exported with solution.
- Permissions can overlap.
- Use Security Configuration wizard to manage roles.

Create a security configuration

© Copyright IBM Corporation 2018

Security Configurations

The Security Configuration wizard provides a quick way to configure security across a solution. With the Security Configuration wizard, you can apply the IBM Case Manager solution configuration correctly and consistently across environments.

When you create a security configuration, you set permissions for roles. A privilege definition document defines the permission settings.

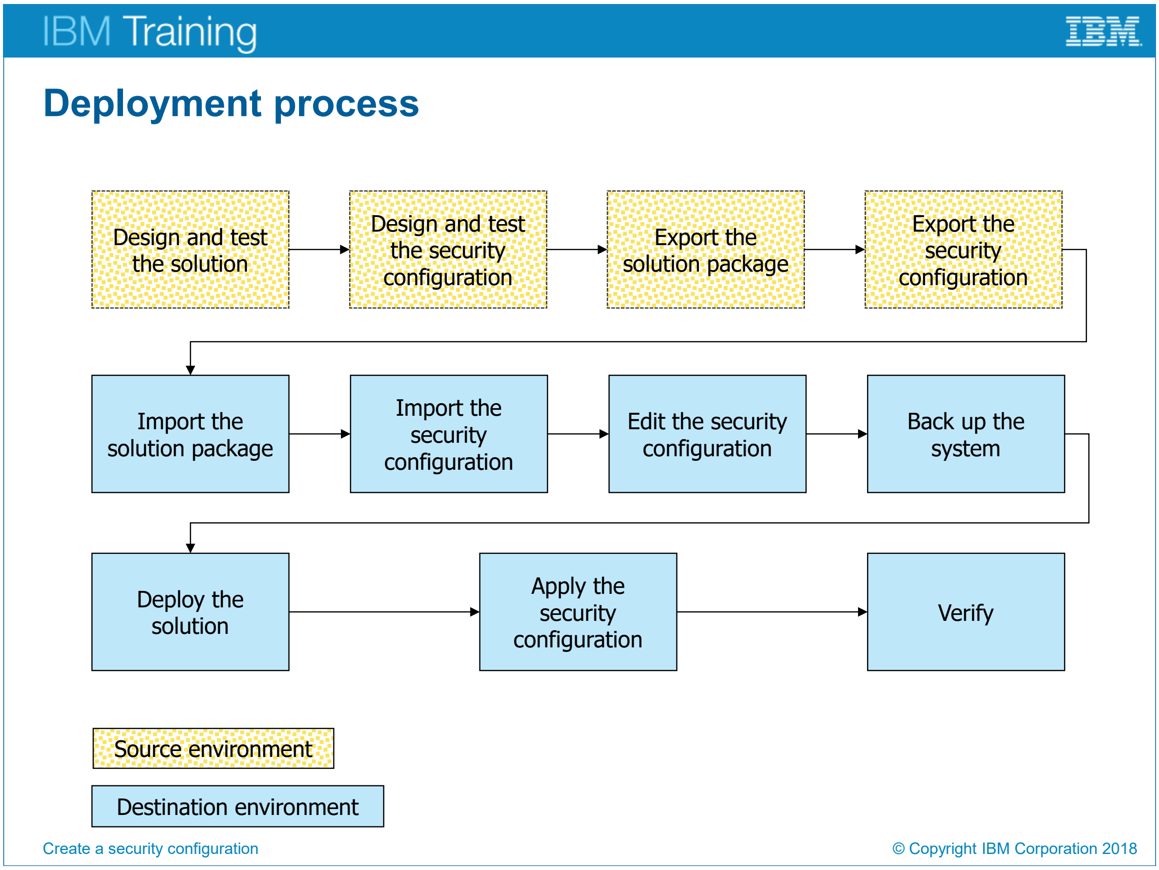
The default permissions are:

- Create Case
- View Case
- Update Case
- Manage Case

The security configuration is exported with the solution, and then applied after the solution is deployed.

Some permissions include other permissions. For example, if you have the Update Case permission, you automatically have View Case permissions.

In a development environment, you can use the Manage Roles button in Case Manager Client, but in other environments, use a security configuration.



IBM Training

Deployment process

Design and test the solution

Design and test the security configuration

Export the solution package

Export the security configuration

Import the solution package

Import the security configuration

Edit the security configuration

Back up the system

Deploy the solution

Apply the security configuration

Verify

Source environment

Destination environment

Create a security configuration

© Copyright IBM Corporation 2018

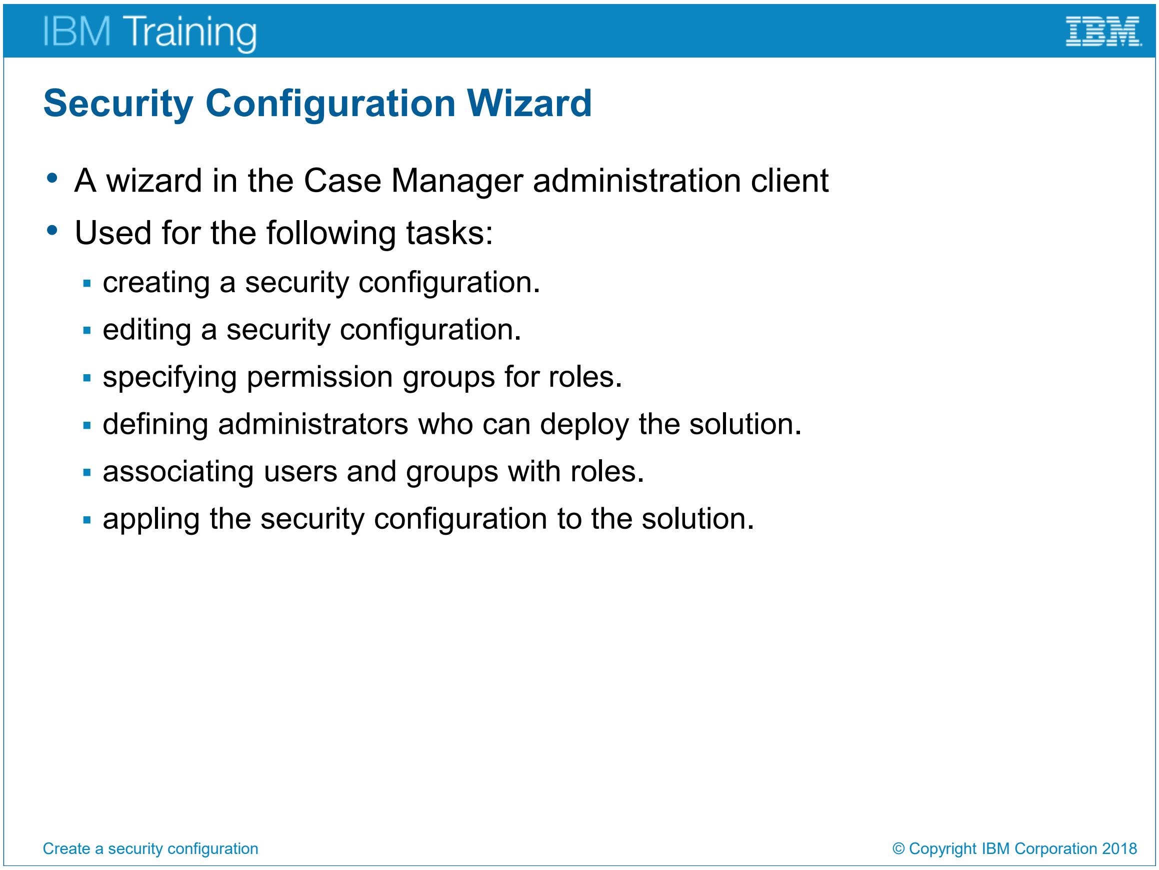
Deployment process

This graphic shows the stages of deploying a solution with a security configuration.

The deployment process must be a repeatable and reliable process.

Part of that deployment process is migrating and applying the Security Configuration.

When the solution is deployed to another environment, the roles and permissions must be mapped to users and groups in the target environment. To accomplish this mapping with a repeatable and reliable procedure, you need to create a security configuration that can be exported with the solution.



IBM Training

Security Configuration Wizard

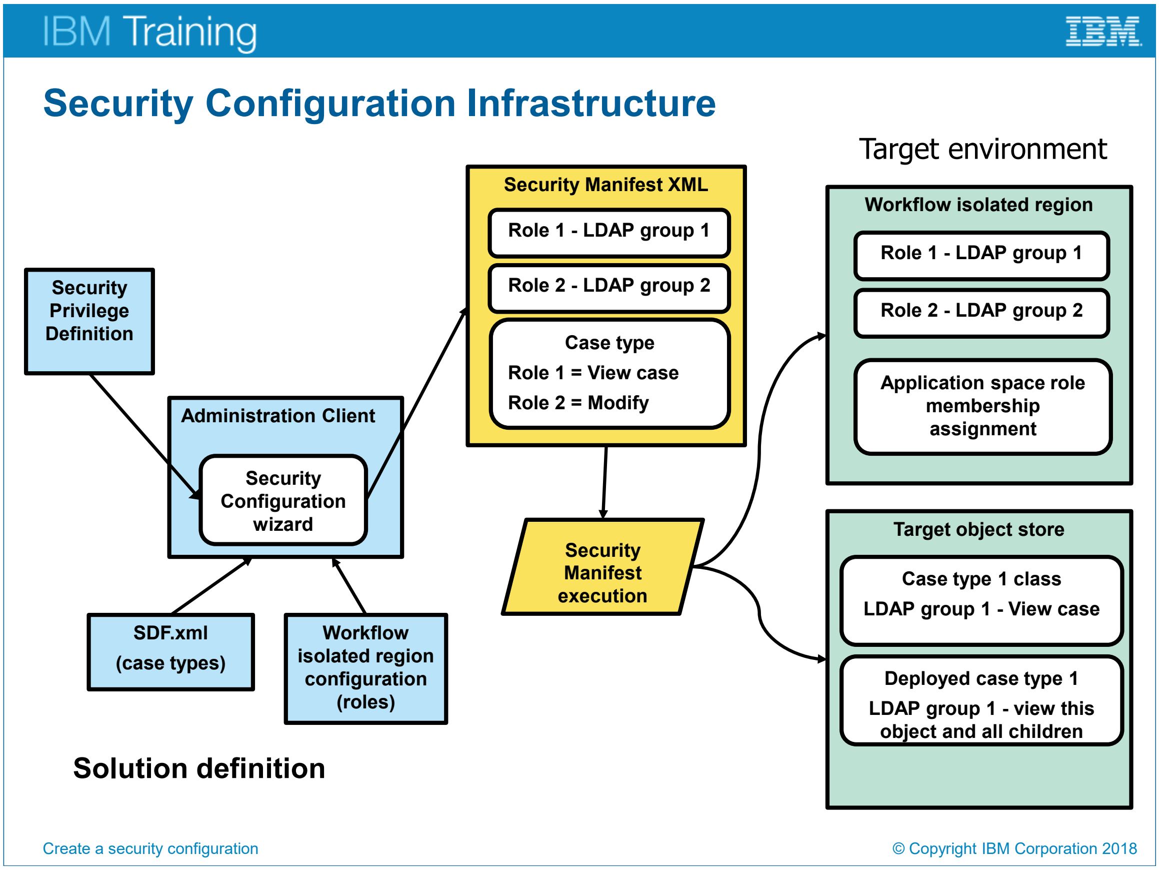
- A wizard in the Case Manager administration client
- Used for the following tasks:
  - creating a security configuration.
  - editing a security configuration.
  - specifying permission groups for roles.
  - defining administrators who can deploy the solution.
  - associating users and groups with roles.
  - appling the security configuration to the solution.

Create a security configuration

© Copyright IBM Corporation 2018

Security Configuration Wizard

You can create security configurations with the Security Configuration wizard. You start the Security Configuration wizard from the Case Manager administration client. You use the Security Configuration Wizard to create a security configuration manifest.



IBM Training

Security Configuration Infrastructure

Target environment

Security Manifest XML

Role 1 - LDAP group 1

Role 2 - LDAP group 2

Case type
Role 1 = View case
Role 2 = Modify

Workflow isolated region

Role 1 - LDAP group 1

Role 2 - LDAP group 2

Application space role membership assignment

Security Privilege Definition

Administration Client

Security Configuration wizard

Security Manifest execution

Target object store

Case type 1 class
LDAP group 1 - View case

Deployed case type 1
LDAP group 1 - view this object and all children

SDF.xml
(case types)

Workflow isolated region configuration (roles)

Solution definition

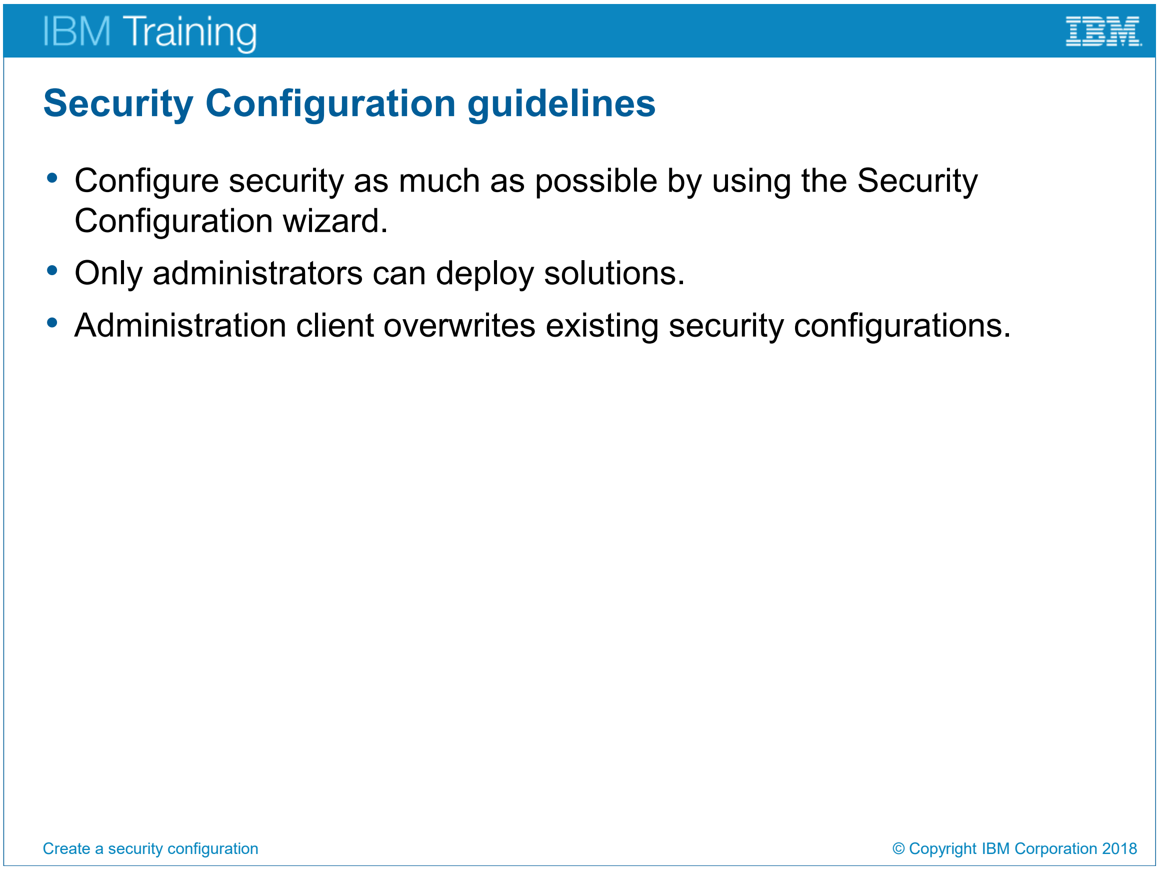
Create a security configuration

© Copyright IBM Corporation 2018

Security Configuration Infrastructure

This graphic shows the structure that underlies the Security Configuration wizard.

You export the solution security configuration as a security configuration file, also called a security configuration manifest. You can reuse this file, and transfer it to multiple environments when you transfer your solution package. In this way, you can package your security configuration as easily as your roles, properties, and workflows.



IBM Training

Security Configuration guidelines

- Configure security as much as possible by using the Security Configuration wizard.
- Only administrators can deploy solutions.
- Administration client overwrites existing security configurations.

Create a security configuration

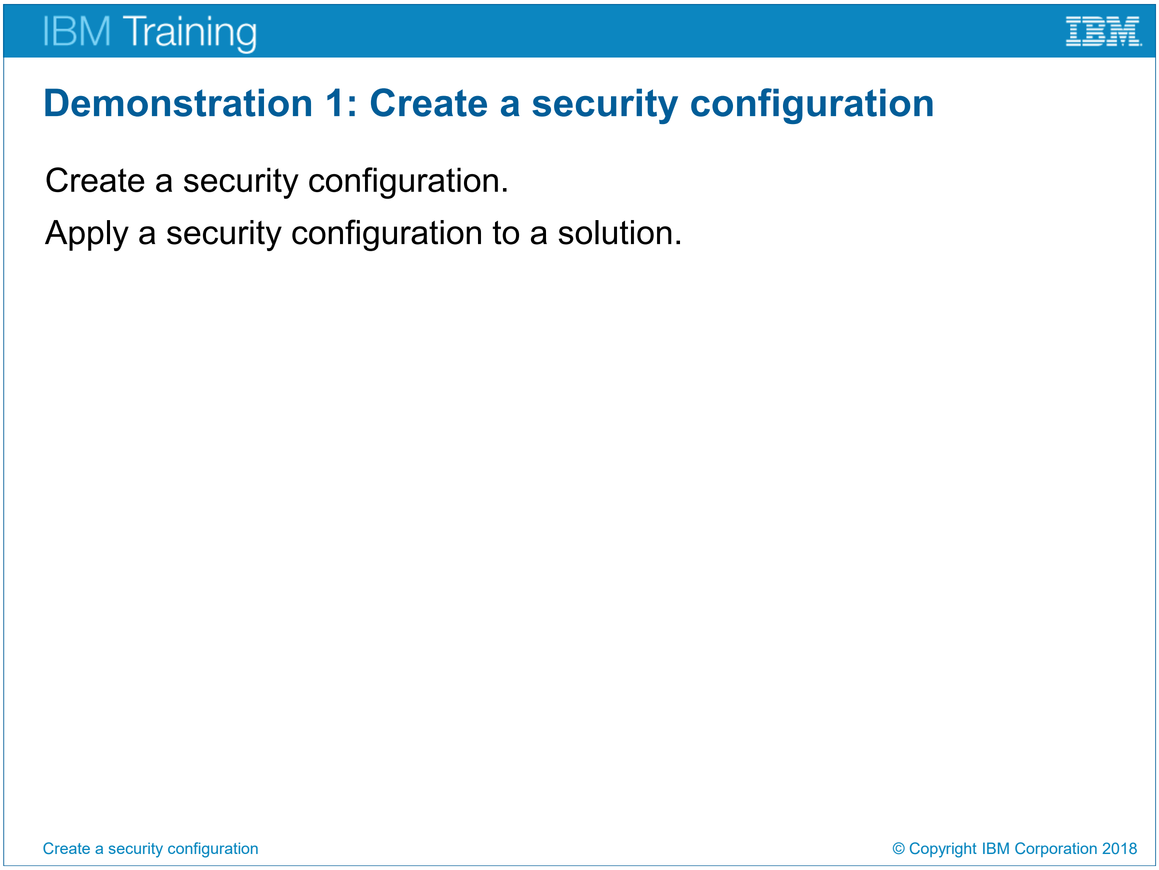
© Copyright IBM Corporation 2018

Security Configuration guidelines

To save time and make the process more efficient, configure security as much as possible by using the Security Configuration wizard. Then, configure any remaining security areas on an individual basis.

Only the users and groups that you add as administrators can redeploy the solution, or reapply a security or audit configuration. Even users who could previously deploy the solution lose this permission if they are not included as administrators in the security configuration manifest. When you create the security configuration file, ensure that anyone who redeploys the solution is configured as an administrator.

When you apply a security configuration, the new security settings overwrite existing security settings.



IBM Training

Demonstration 1: Create a security configuration

Create a security configuration.

Apply a security configuration to a solution.

Create a security configuration

Demonstration 1: Create a security configuration

Demonstration 1: Create a security configuration

Purpose:
You create security configurations to manage role security in a solution. After you create the security configuration manifest, you apply it to a solution. When you export the solution package, you also export the solution configuration manifest.

Case Manager Builder URL: **http://vclassbase:9081/CaseBuilder**

Case Manager Client URL: **http://vclassbase:9081/navigator/?desktop=icm**

Case Manager Admin URL: **http://vclassbase:9081/navigator/?desktop=icmadmin**

Solution builder Username/password: **Paula/FileNet1**

Task 1. Start the Security Configuration Wizard.

1. Start **Firefox**.
2. Click the **Case Admin** shortcut on the home page.
3. Log in as **Paula/FileNet1**.
4. Open the **DEV_design** object store.
5. Click **DEV_design** > **Solutions**.
6. Select the **Medical Visit** solution in the main panel.
7. Click **Actions** > **Manage** > **Security Configuration**.

   You can also right-click the solution to get to the same menu options.

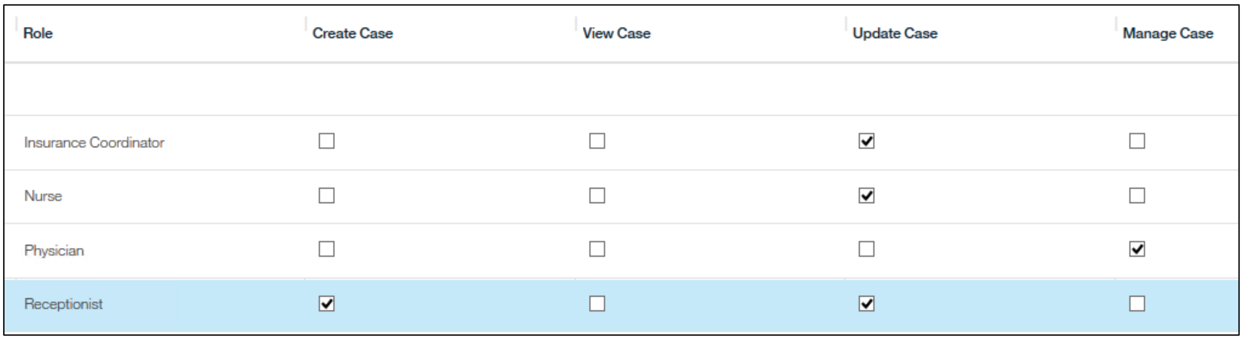
Task 2. Create a security configuration.

1. On the **Create or edit a security configuration** page, select **Create a security configuration**, then click **Next**.
2. On the **Name the security configuration** page, type `MEDSEC` in the **Security manifest name** field, then click **Next**.

3. On the **Modify permissions for roles** page, select the following permissions, then click **Next**:

    - **Insurance Coordinator: Update Case**
    - **Nurse: Update Case**
    - **Physician: Manage Case**
    - **Receptionist: Create Case, Update Case**

    The results appear as follows:



Role	Create Case	View Case	Update Case	Manage Case
Insurance Coordinator	□	□	☑	□
Nurse	□	□	☑	□
Physician	□	□	□	☑
Receptionist	☑	□	☑	□

    The order in which the roles are displayed is not important.

4. On the **Define the administrators and assign privileges** page, verify that **Paula** is listed, and then add **P8admin**, then click **Next**.
5. On the **Associate users and groups with roles** page, select the role, and then click **Add**, then use the **Add users and groups to role** wizard to add the following users to their roles:

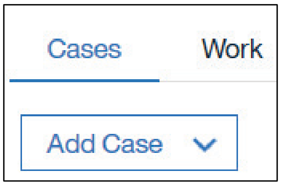
    - **Insurance Coordinator: Addington**
    - **Nurse: Sue**
    - **Receptionist: Cody**
    - **Physician: Fred**

    After you add users to a role, you can expand ▸ the role to see the assignments.

6. Click **Next**.
7. On the **Apply the security configuration** page, select **Apply the security configuration**, click **Save**, then click **Apply**.
8. Verify that you receive a success message at the bottom of the window, then click **Close**.
9. Log out of **Case Manager Administration Client**, then close **Firefox**.

Task 3. Create a case to verify security settings

1. Use **Firefox** to log on to **Case Manager Client** as **Cody/FileNet1**.
2. In the top right of the page, select the **Medical Visit** solution, **Receptionist** role.
3. Open the **Cases** tab.
4. Confirm that the **Add Case** button is active.



5. Click **Add Case** > **Office Visit**.
6. Type a client name, `Smith`, then click **Add**.

   Cody has access to the Receptionist role because Cody was associated with this role in the security configuration wizard.

Task 4. Complete the Sign in step.

1. Open the **Work** tab.
2. Confirm that the in-basket name is **Receptionist**.
3. Open the **Sign In** work item.
4. Click **Complete**.
5. Log out of **Case Manager Client**.

Task 5. Complete the Check insurance step.

1. Log on to **Case Manager Client** as **Addington/FileNet1**.
2. Select the **Medical Visit** > **Insurance Coordinator** role.
3. Verify that the **Add Case** button is disabled.
4. Click the **Work** tab. Verify that the in-basket is named **Insurance Coordinator**.
5. Open and complete the **Check Insurance** work item.
6. Log out of **Case Manager Client**.

Task 6. Complete the Collect Copay step.

1. Log on to **Case Manager Client** as **Cody/FileNet1**.
2. Open the **Work** page.
3. Open and complete the **Collect Copay** work item.
4. Log out of **Case Manager Client**.

Task 7. Complete the Get Vitals step.

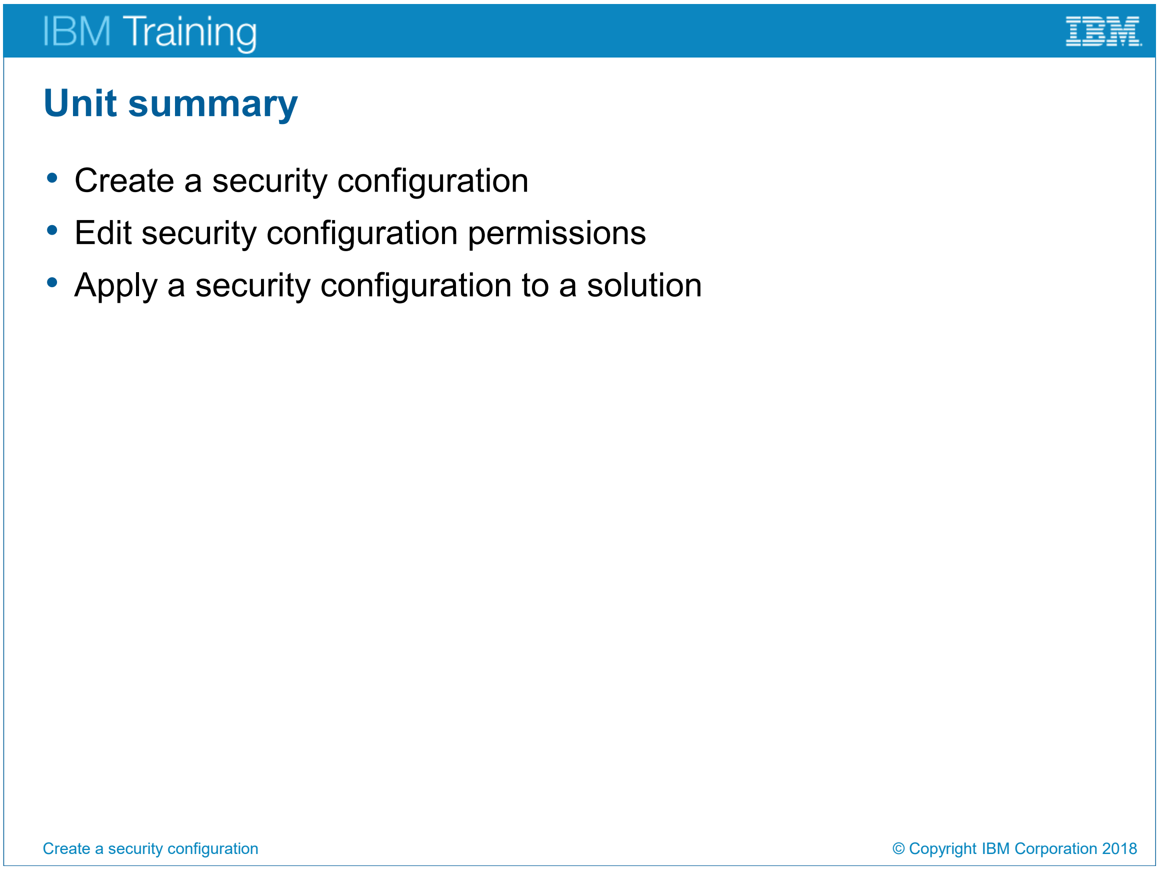
1. Log on to **Case Manager Client** as **Sue/FileNet1**.
2. Select the **Medical Visit** > **Nurse** role.
3. Open the **Work** tab.
4. Verify that the in-basket name is **Nurse**.
5. Open and complete the **Get Vitals** work item.
6. Log out **of Case Manager Client**.

Task 8. Complete the Consultation step.

1. Log in to **Case Manager Client** as **Fred/FileNet1**.
2. Select the **Medical Visit** > **Physician** role.
3. Open the **Work** tab.
4. Open and complete the **Consultation** step.
5. Log out of **Case Manager Client**.
6. Close all browsers.

Result:

You created and applied a security configuration to a solution.



IBM Training

Unit summary

- Create a security configuration
- Edit security configuration permissions
- Apply a security configuration to a solution

Create a security configuration

© Copyright IBM Corporation 2018

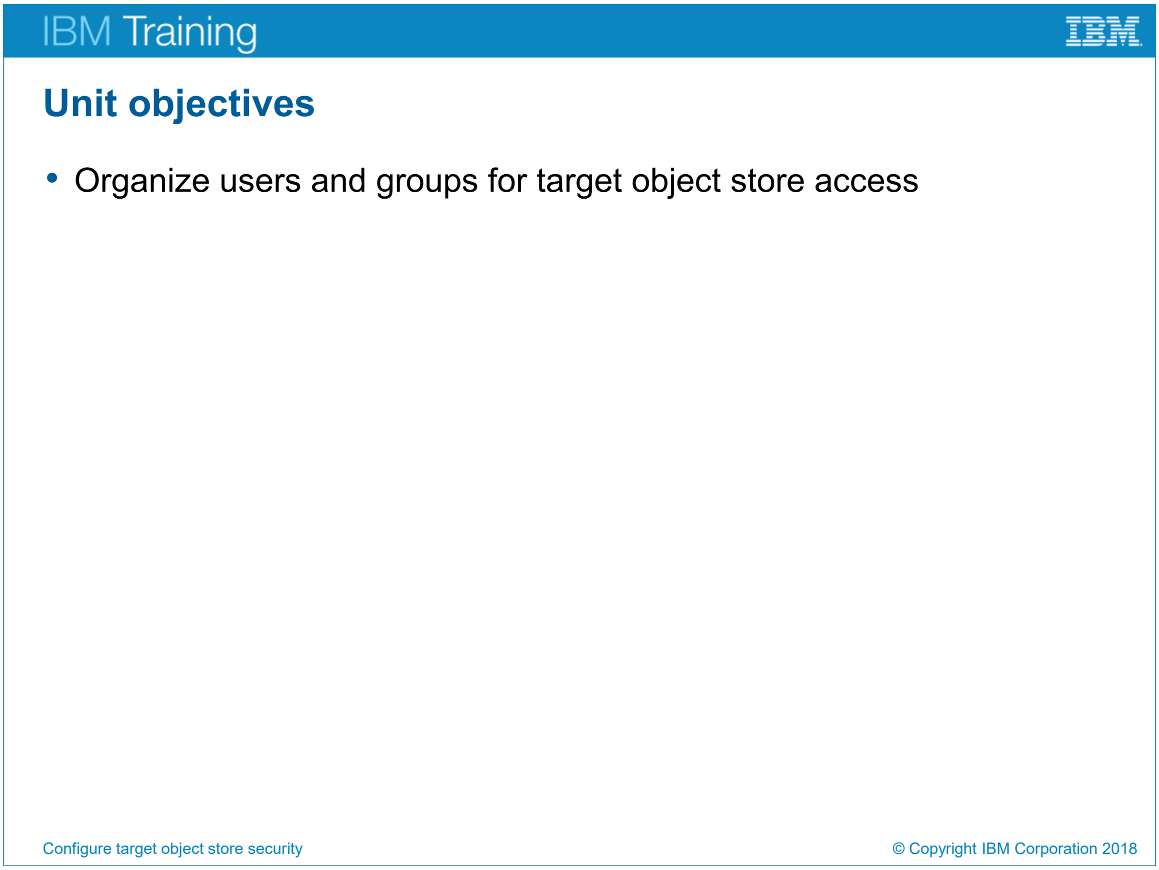
Unit summary

Unit 5 Configure target object store security

IBM Training

Configure target object store security

IBM Case Manager V5.3.2



IBM Training

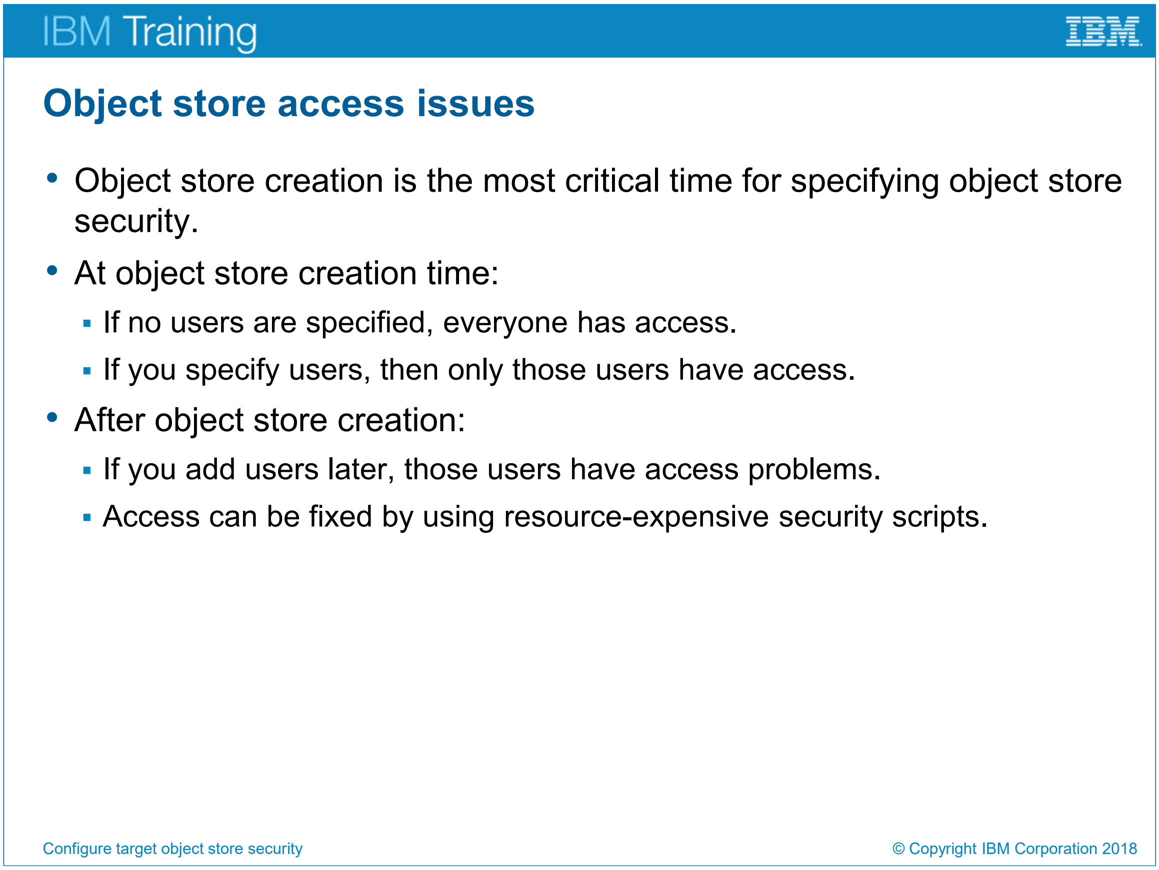
Unit objectives

- Organize users and groups for target object store access

Configure target object store security

© Copyright IBM Corporation 2018

Unit objectives



IBM Training

Object store access issues

- Object store creation is the most critical time for specifying object store security.
- At object store creation time:
  - If no users are specified, everyone has access.
  - If you specify users, then only those users have access.
- After object store creation:
  - If you add users later, those users have access problems.
  - Access can be fixed by using resource-expensive security scripts.

Configure target object store security

© Copyright IBM Corporation 2018

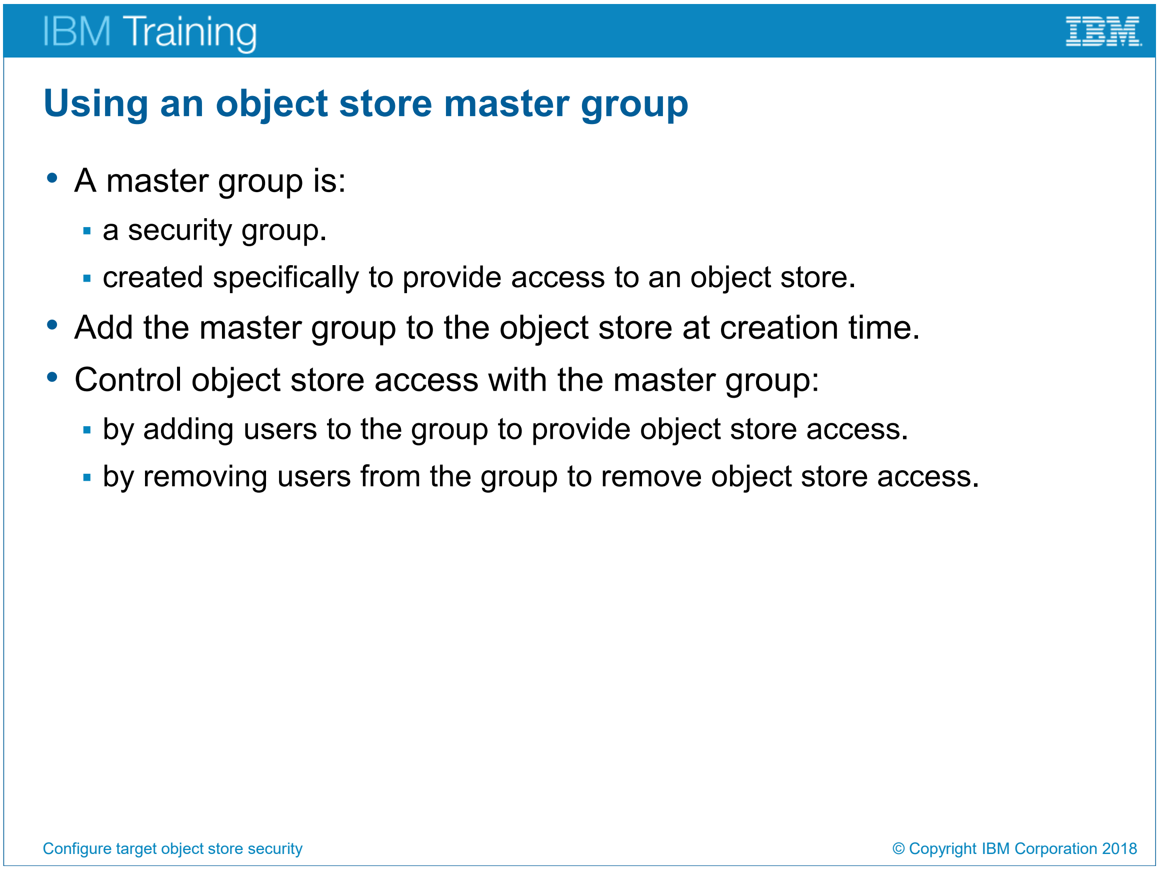
Object store access issues

The object store creation wizard provides the means to set security for the object store. You specify the users who have administration rights and the users who have default access. If you leave the default users field blank, the object store is created with default access given to #AUTHENTICATED-USERS. Anyone who can log on has view rights to all objects by default, which makes the system unsecured.

If you specify a user or group, then all other users and groups are denied access to the object store and the object store is secure. However, you might have new users joining the company who must access the object store. If you add those users directly to the object store with default access, they still have access problems. Object store access does not automatically grant access to existing objects in the object store, including class definitions, documents, and properties. Each object on the object store has its own access control list in which the new user is not included.

An object store administrator can run a security script wizard tool that updates objects on the object store. This tool, is resource-expensive, however. The more objects that are on the object store, the longer this tool takes to update security.

Fortunately, there is a much easier way to manage object store security after object store creation: master groups.



IBM Training

Using an object store master group

- A master group is:
  - a security group.
  - created specifically to provide access to an object store.
- Add the master group to the object store at creation time.
- Control object store access with the master group:
  - by adding users to the group to provide object store access.
  - by removing users from the group to remove object store access.

Configure target object store security

Using an object store master group

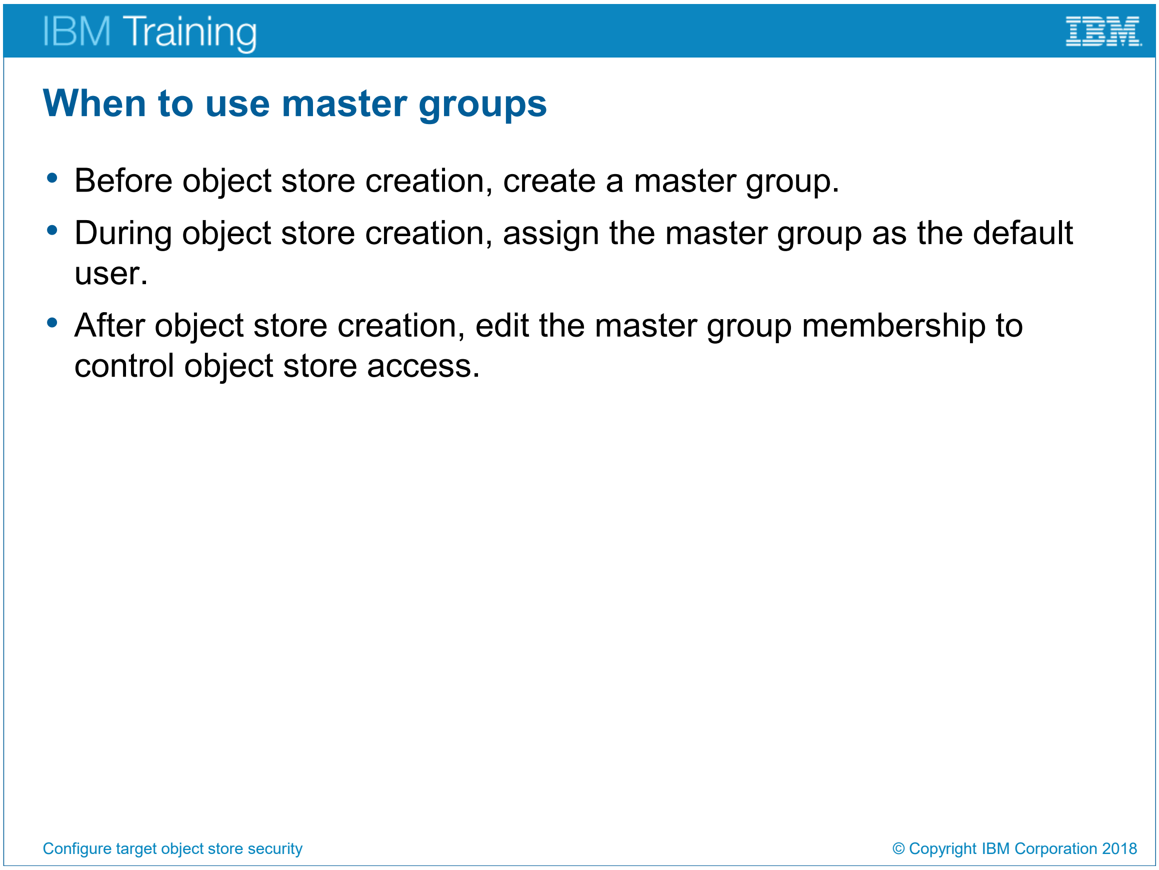
A master group is a security group that is created specifically to provide access to an object store or group of object stores. You control access to the object store by controlling the membership of the master group. Master groups are also sometimes known as super groups.

Use a master group to avoid the following problems:

- Object store access is unrestricted.
- Users do not have access to objects that were created before the user was added to the object store.

The master group has default access rights to all object store objects. Anyone who is added to the master group at any time, therefore, has default access to all object store objects.

Access can be further refined with other groups.



IBM Training

When to use master groups

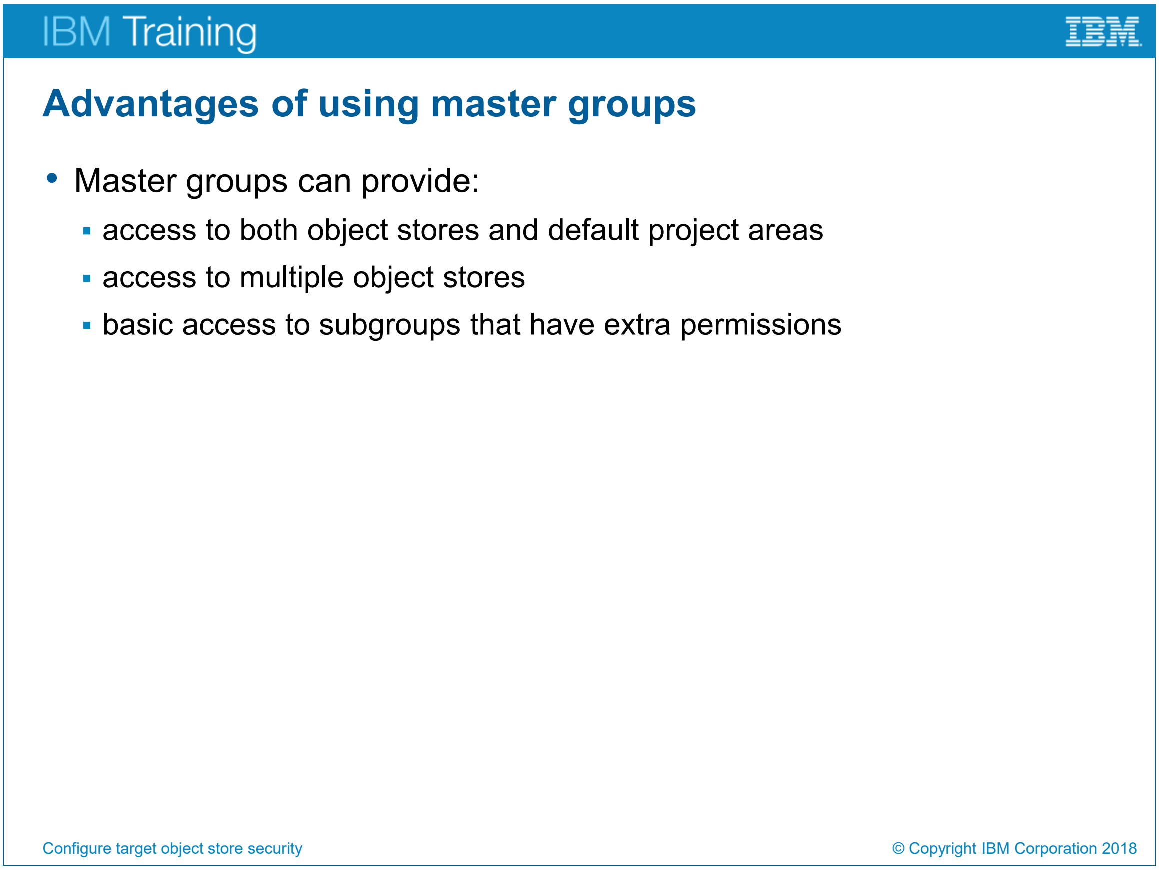
- Before object store creation, create a master group.
- During object store creation, assign the master group as the default user.
- After object store creation, edit the master group membership to control object store access.

Configure target object store security

© Copyright IBM Corporation 2018

When to use master groups

Although adding a new user to an object store does not add permissions on existing objects, adding a user to an LDAP group that already has access to the objects does. By specifying a master group at object store creation time, you can always add users and groups to the object store later and ensure that they have access to all existing objects. However, the group must exist before the object store is created so that you can add the group to the default users list when you create the object store.



IBM Training

Advantages of using master groups

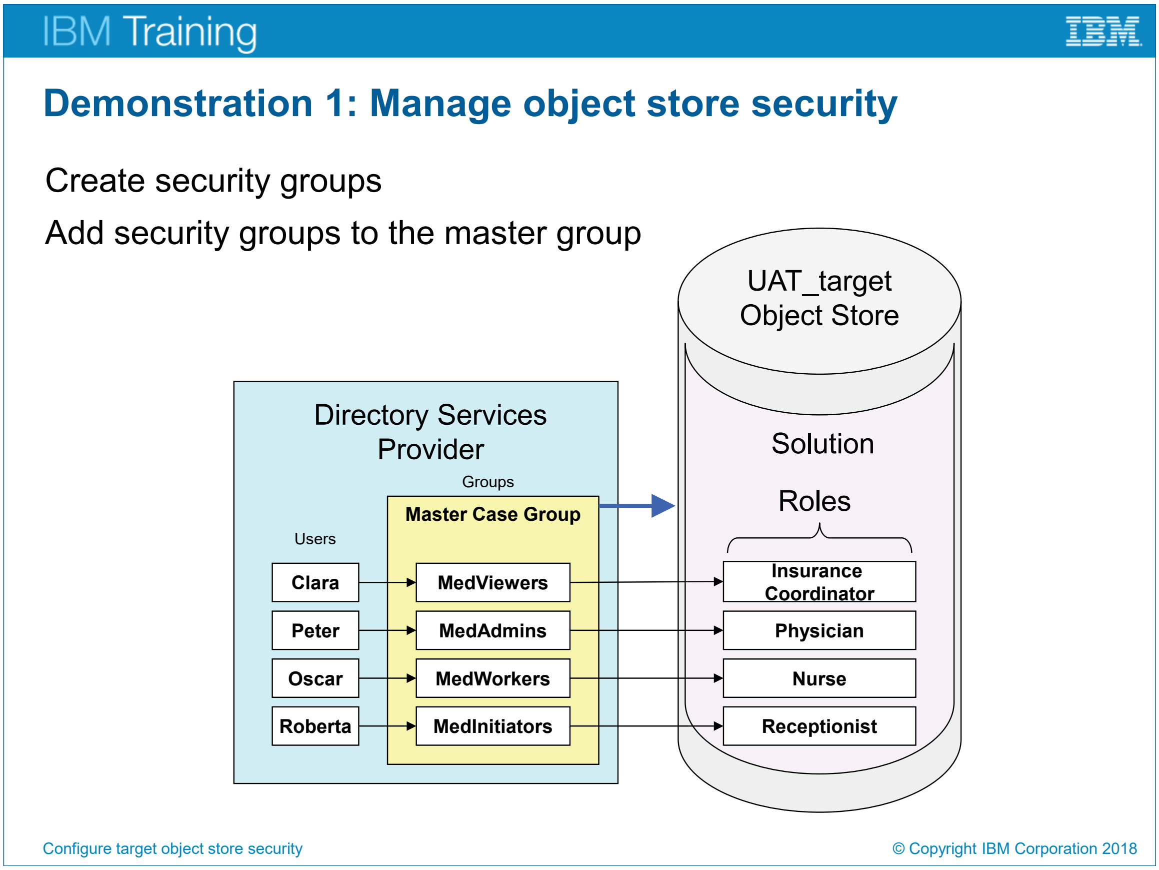
- Master groups can provide:
  - access to both object stores and default project areas
  - access to multiple object stores
  - basic access to subgroups that have extra permissions

Configure target object store security

© Copyright IBM Corporation 2018

Advantages of using master groups

Most security services allow groups to be added to other groups, so you might have a master group for object store access, then add other groups to this master group to add many users at a time or to provide extra permissions.



IBM Training

Demonstration 1: Manage object store security

Create security groups

Add security groups to the master group

Directory Services Provider

Groups

Master Case Group

Users

Clara → MedViewers → Insurance Coordinator

Peter → MedAdmins → Physician

Oscar → MedWorkers → Nurse

Roberta → MedInitiators → Receptionist

UAT_target Object Store

Solution

Roles

Configure target object store security

© Copyright IBM Corporation 2018

Demonstration 1: Manage object store security

The graphic shows the relationship between case manager groups, the object store master group, and the roles within the solution. The Master Case Group provides default object store access. Several groups are added to the Master Case Group to supply roles with users.

Demonstration 1: Manage object store security

Purpose:
The Medical Visit solution is going to be moved to a new environment for user acceptance tests. Before the solution is transferred, you, the system administrator, must ensure that the target object store security is set up properly to prevent user access problems. Your student system has two environments: a Development environment and a UAT environment. You are going to configure object store security for the UAT environment.

Case Manager Admin URL: **http://vclassbase:9081/navigator/?desktop=icmadmin**

Administration Client for Content Platform Engine URL: **http://vclassbase:9080/acce/**

UAT Case Client URL: **http://vclassbase:9082/UAT_ICN/?desktop=icm**

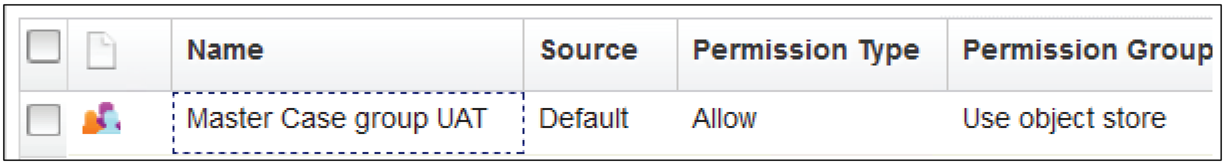
Administrator Username: **p8admin**

Administrator Password: **FileNet1**

Task 1. Inspect object store security.

The target object store has already been created. To make sure that it can provide proper access, you are going to inspect the security settings.

1. Start **Firefox**, then click the **ACCE** link to log in to **Administration Console for Content Platform Engine** as **p8admin/FileNet1**.
2. In the Navigation pane, expand the **Object Stores** node if it is not already expanded.
3. Select the object store: **UAT_target**.
4. Open the **Security** tab.
5. Confirm that **Master Case group UAT** has **Use object store** permissions.



□		Name	Source	Permission Type	Permission Group
□		Master Case group UAT	Default	Allow	Use object store

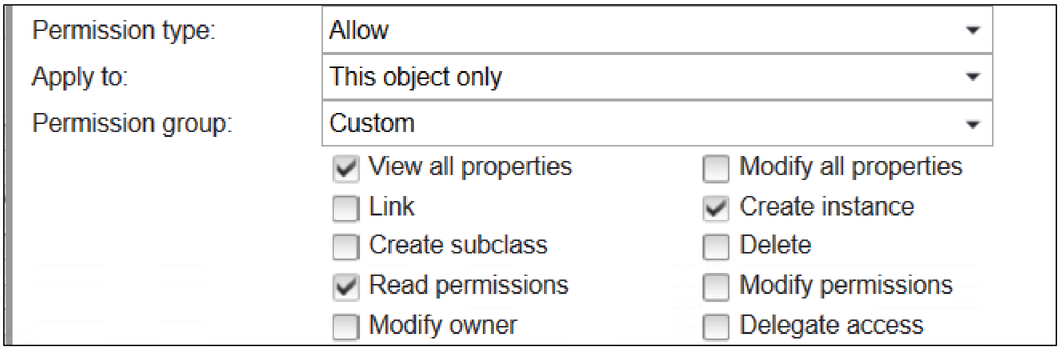
Task 2. Inspect data design security.

1. In the Navigation pane expand **Data Design** > **Classes**.
2. Select **Custom Object**.
3. Open the **Security** tab.
4. Confirm that **Master Case group UAT** has **Custom** permissions to custom objects.

5. Check the box beside to **Master Case group UAT** ☑, then click **Edit**.
6. On the **Edit Permissions** dialog, confirm that the following permissions are checked:

   - **View all properties**
   - **Read permissions**
   - **Create instance**

   The results appear as follows:



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
☐ Delegate access

   Do not change these security settings.

7. Click **Cancel**.
8. Use the previous steps (3-7) to ensure that **Master Case group UAT** has the same permissions for the **Document** and **Folder** classes.
9. Log out of **Administration Client for Content Platform Engine** and close **Firefox**.

Task 3. Start Active Directory.

1. On the Windows menu bar, click the **Windows** button ⊞.
2. Click **Administrative Tools**.
3. Double-click **Active Directory Users and Computers**.

Task 4. Create Active Directory groups.

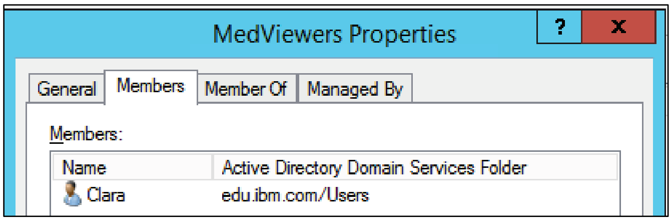
1. Click **New Group** .
2. Type the group name, `MedViewers`.
3. Click **OK**.
4. Create the following three groups by using steps 1-3.

   - **MedWorkers**
   - **MedAdmins**
   - **MedInitiators**

Task 5. Add users to groups.

1. In **Active Directory Users and Computers**, double-click the **MedViewers** group.
2. Open the **Members** tab.
3. Click Add.
4. In the object name box, type **`Clara`**, then click **Check Names**. Click **OK**.

   The results appear as follows:



Members:

Name	Active Directory Domain Services Folder
Clara	edu.ibm.com/Users

5. Click **OK** to close the **MedViewers** group.
6. Use the previous steps (1-5) to add each of the following users to the indicated group:
   - **MedAdmins: Peter**
   - **MedWorkers: Oscar**
   - **MedInitiators: Roberta**

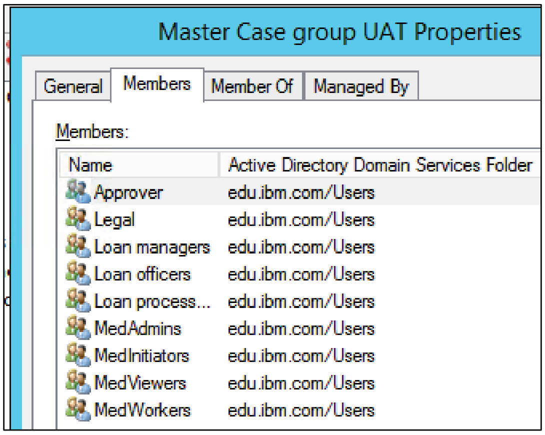
Task 6. Add groups to Master Case UAT group.

The users do not have access to the object store until they are included in the Master Group UAT. You are going to add groups to the Master Group UAT to provide all members of those groups default object store access.

1. In **Active Directory Users and Computers**, open **Master Case group UAT**.
2. Open the **Members** tab.
3. Click **Add**.
4. Type **`Med`**, then click **Check Names**.

5. Select all four groups, then click **OK**.

   The results appear as follows:



Members:

Name	Active Directory Domain Services Folder
Approver	edu.ibm.com/Users
Legal	edu.ibm.com/Users
Loan managers	edu.ibm.com/Users
Loan officers	edu.ibm.com/Users
Loan process...	edu.ibm.com/Users
MedAdmins	edu.ibm.com/Users
MedInitiators	edu.ibm.com/Users
MedViewers	edu.ibm.com/Users
MedWorkers	edu.ibm.com/Users

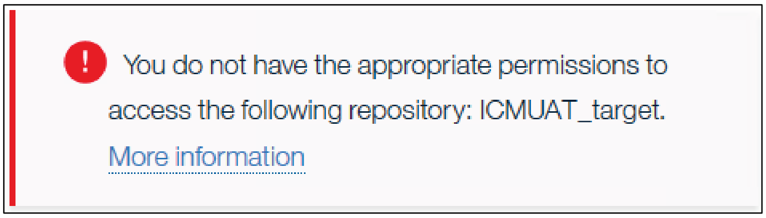
6. Click **OK** to close **Master Case group UAT** properties.
7. Close **Active Directory Users and Computers**.

Task 7. Test object store access.

Before you log in successfully, you are going to log in with an unauthorized account to see what a failed login attempt looks like.

1. Open **Firefox**. On the Home page, click the **UAT Case Client** link.
2. Attempt to log in as **Burt/FileNet1**.
3. Confirm log in failure.

   The results appear as follows:

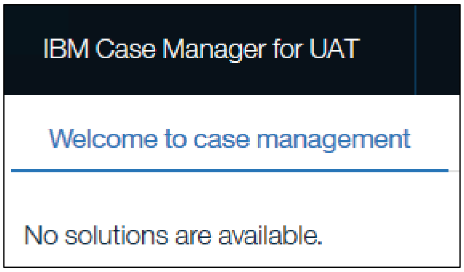


! You do not have the appropriate permissions to access the following repository: ICMUAT_target.

More information

4. Log in as **Clara/FileNet1**. Confirm that login is successful.

   The results appear as follows:



IBM Case Manager for UAT

Welcome to case management

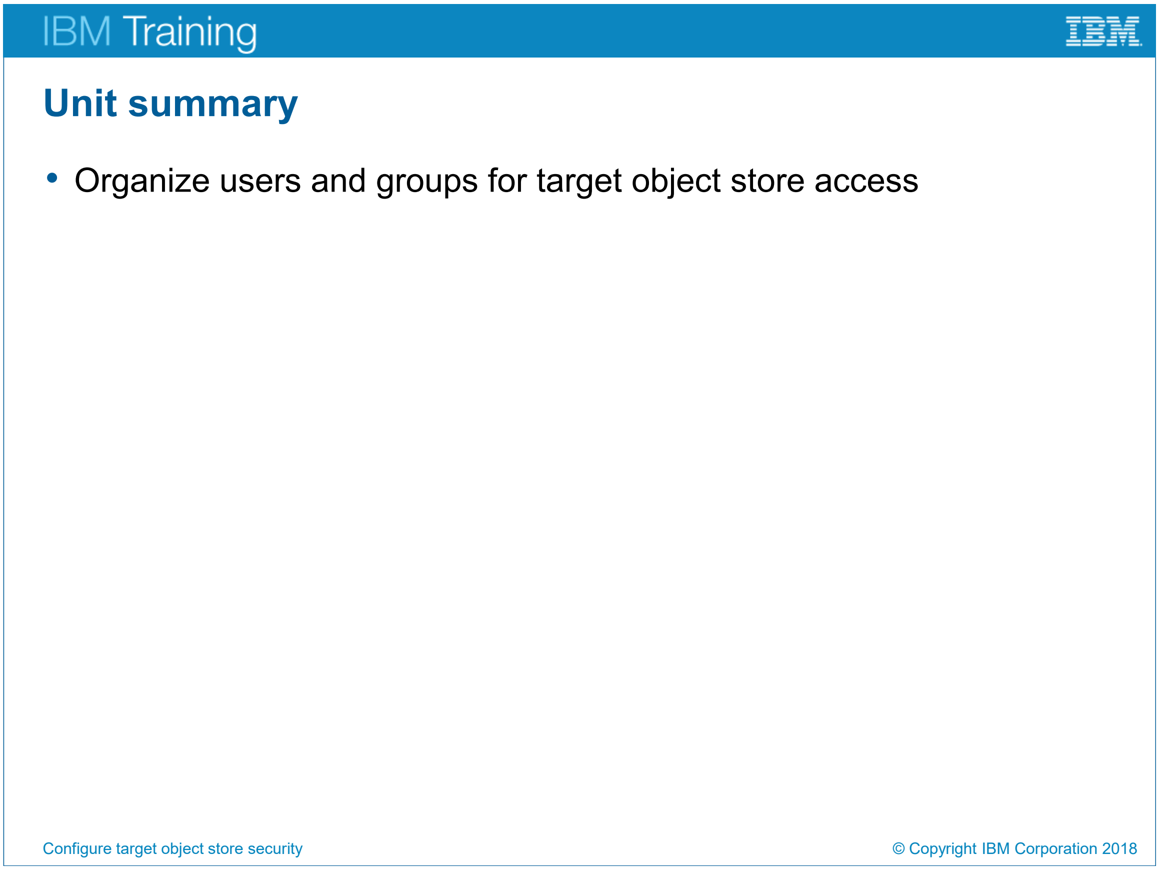
No solutions are available.

5. Log out of **Case Manager Client**.

6. Confirm that you can successfully log in with each of these accounts:
   - **Peter/FileNet1**
   - **Oscar/FileNet1**
   - **Roberta/FileNet1**
7. Log out of all applications and close all browsers.

Results:

You created case user groups and added them to the master group to give the users default object store access. You used nested groups to provide group access to the object store that are consistent with future role assignments.



IBM Training

Unit summary

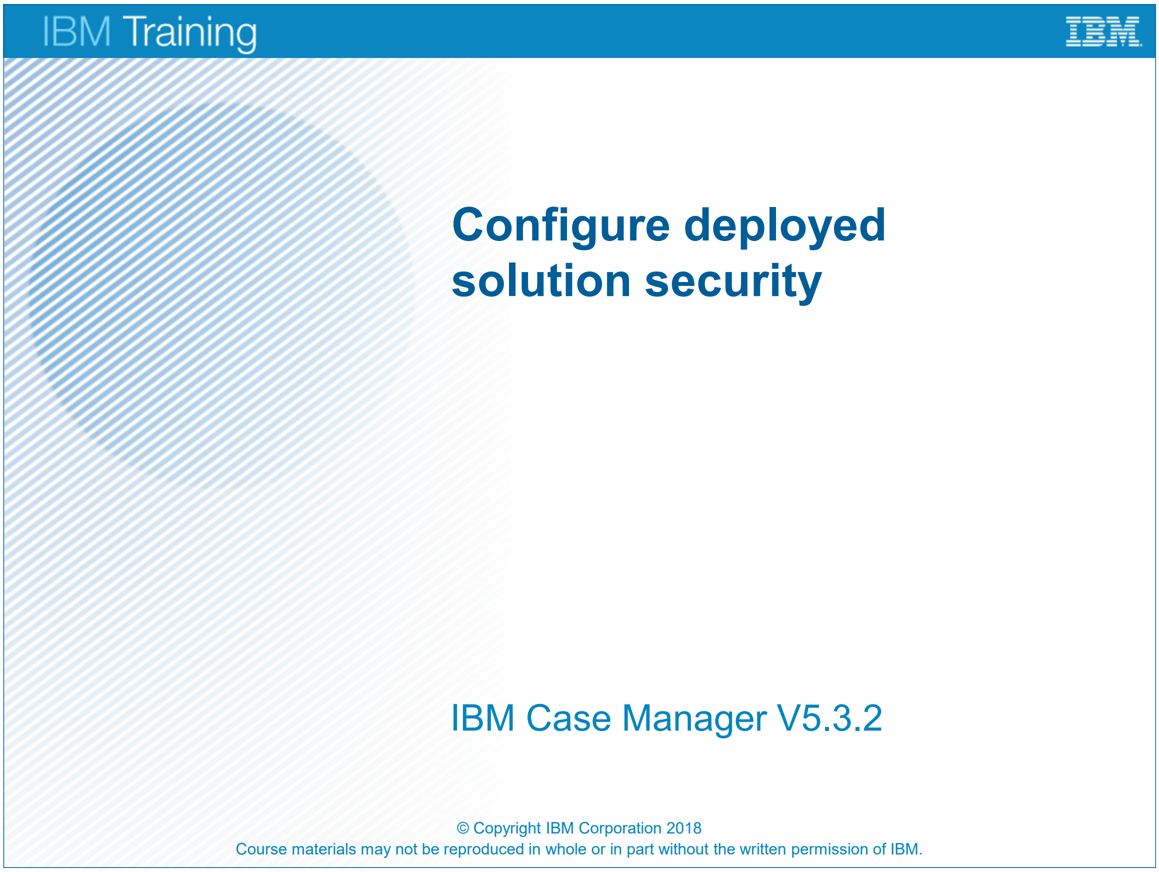
- Organize users and groups for target object store access

Configure target object store security

© Copyright IBM Corporation 2018

Unit summary

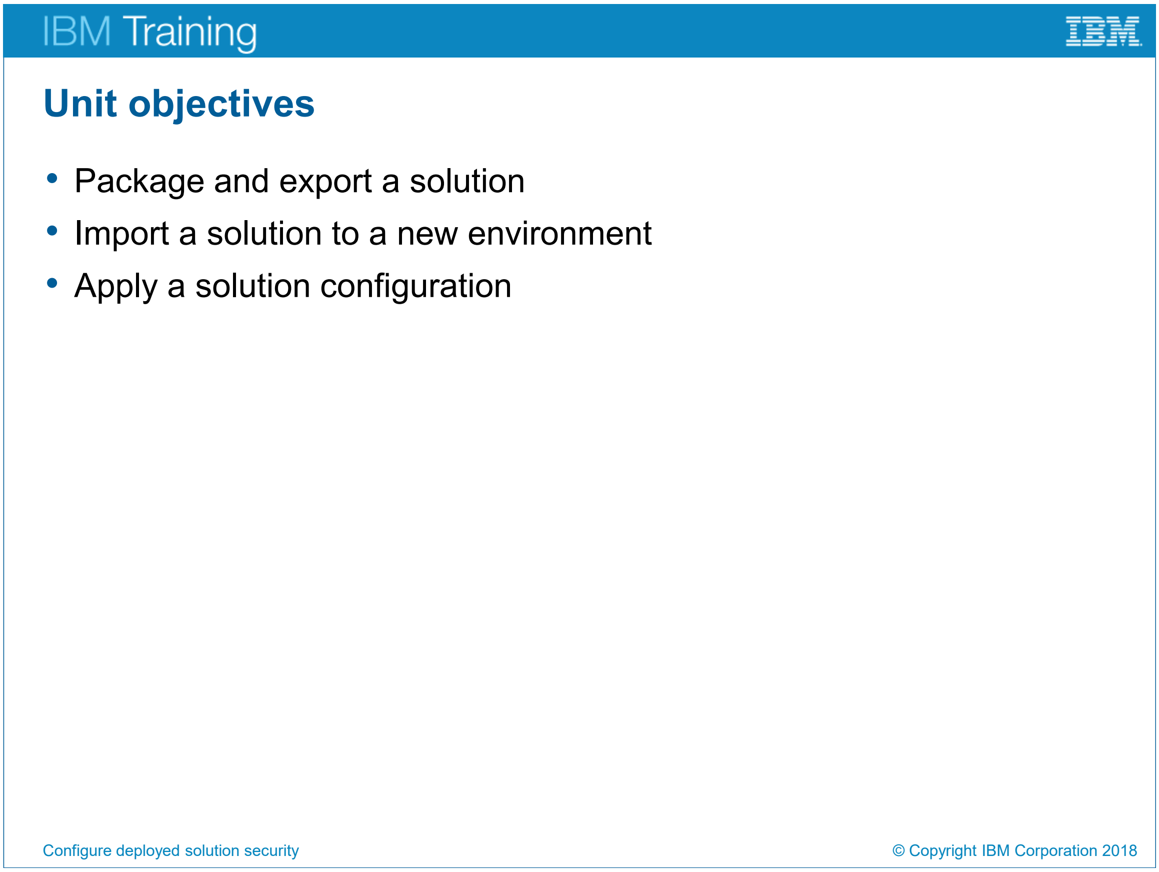
Unit 6 Configure deployed solution security



IBM Training

Configure deployed solution security

IBM Case Manager V5.3.2



IBM Training

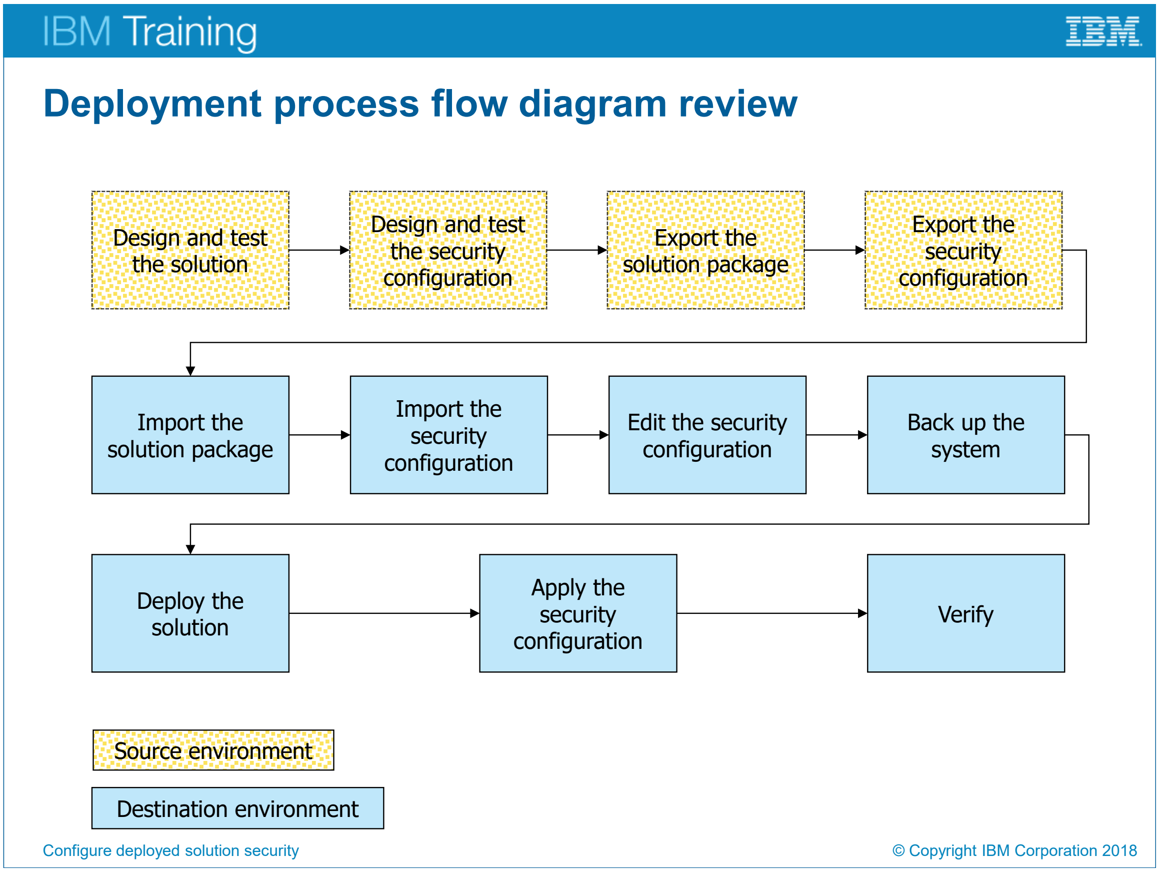
Unit objectives

- Package and export a solution
- Import a solution to a new environment
- Apply a solution configuration

Configure deployed solution security

© Copyright IBM Corporation 2018

Unit objectives



IBM Training

Deployment process flow diagram review

Design and test the solution

Design and test the security configuration

Export the solution package

Export the security configuration

Import the solution package

Import the security configuration

Edit the security configuration

Back up the system

Deploy the solution

Apply the security configuration

Verify

Source environment

Destination environment

Configure deployed solution security

© Copyright IBM Corporation 2018

Deployment process flow diagram review

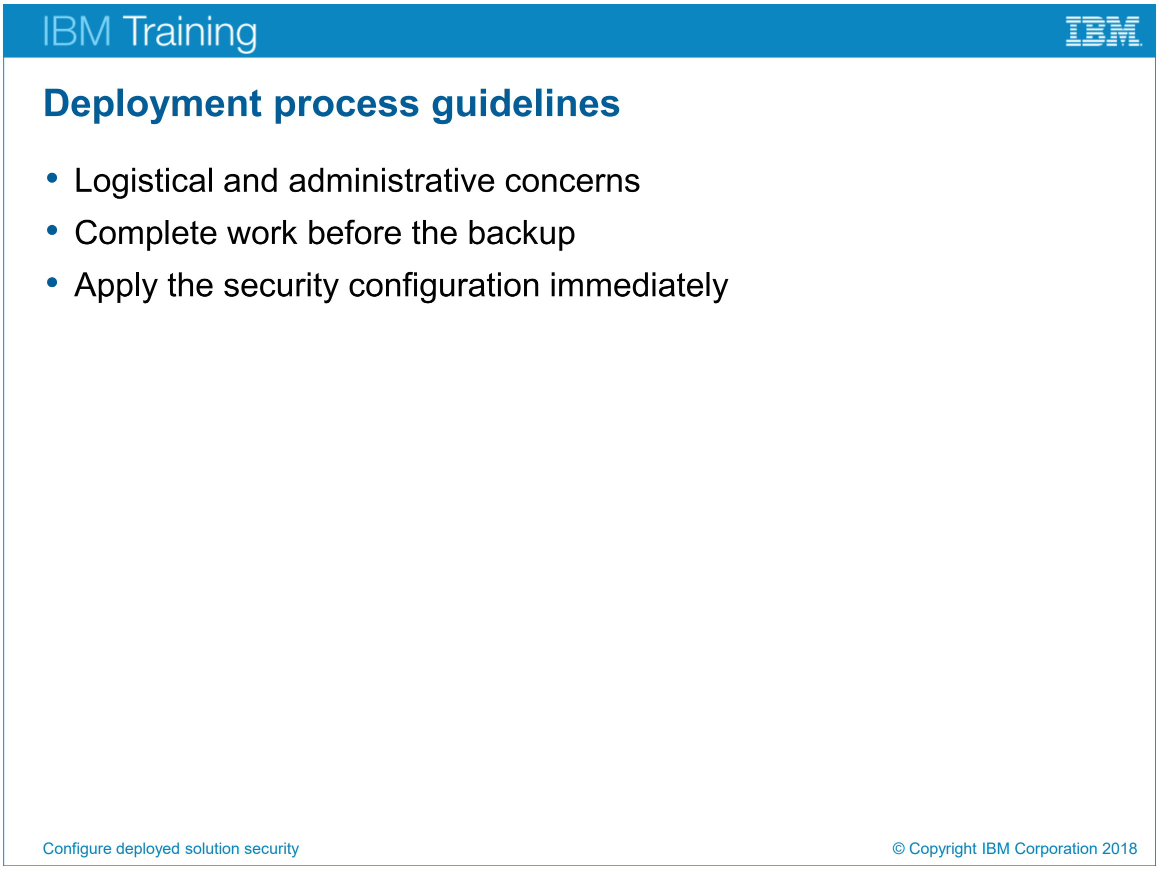
The graphic shows a simple deployment process.

When you export the security configuration, you create a solution configuration package file, sometimes called a security configuration manifest. After you design and test the solution and the security configuration, you export the solution package and the security configuration. The solution in this process includes only assets that were created in Case Manager Builder, so all solution assets can be exported with the Case Manager administration client.

In the destination environment, you import the solution package and the security configuration. You edit the security configuration before you apply it because the new environment has a different set of users and groups that must be mapped to roles.

To avoid as much rework as possible, it is useful to complete as much preparation as you can and then back up the system before you deploy the solution. Exit the security configuration wizard after you save the configuration, but before you apply the configuration to the solution, so that the configuration is saved before you back up the system.

After you complete the previous steps, you can deploy the solution. Apply the security configuration after you deploy the solution so that you can ensure the solution is secure shortly after it is deployed. After you apply the security configuration, verify the solution functionality in the new environment, using the new users and groups.



IBM Training

Deployment process guidelines

- Logistical and administrative concerns
- Complete work before the backup
- Apply the security configuration immediately

Configure deployed solution security

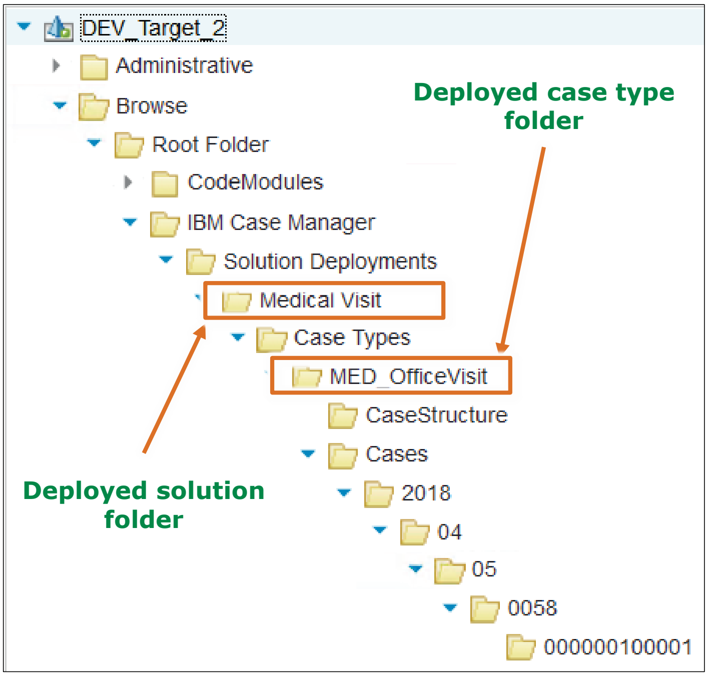
Deployment process guidelines

Use these guidelines when you migrate a solution:

- Logistical and administrative concerns take precedence over efficiency of steps. For example, it might seem more efficient to deploy the solution, then import, edit, and apply the security configuration. However, to maximize the work prior to backing up the target environment, you can edit the security configuration before deployment.
- Minimize the amount of work to do on the server between backup and completion so that the backup is not stale. Perform as many operations as possible before the backup.
- After a solution is deployed, it can be accessed. For maximum security, apply the security configuration immediately after the solution is deployed.

IBM Training

Folder structure and inheritance



- DEV_Target_2
  - Administrative
  - Browse
    - Root Folder
      - CodeModules
      - IBM Case Manager
        - Solution Deployments
          - Medical Visit
            - Case Types
              - MED_OfficeVisit
                - CaseStructure
                - Cases
                  - 2018
                    - 04
                      - 05
                        - 0058
                          - 000000100001

Deployed case type folder

Deployed solution folder

Configure deployed solution security

© Copyright IBM Corporation 2018

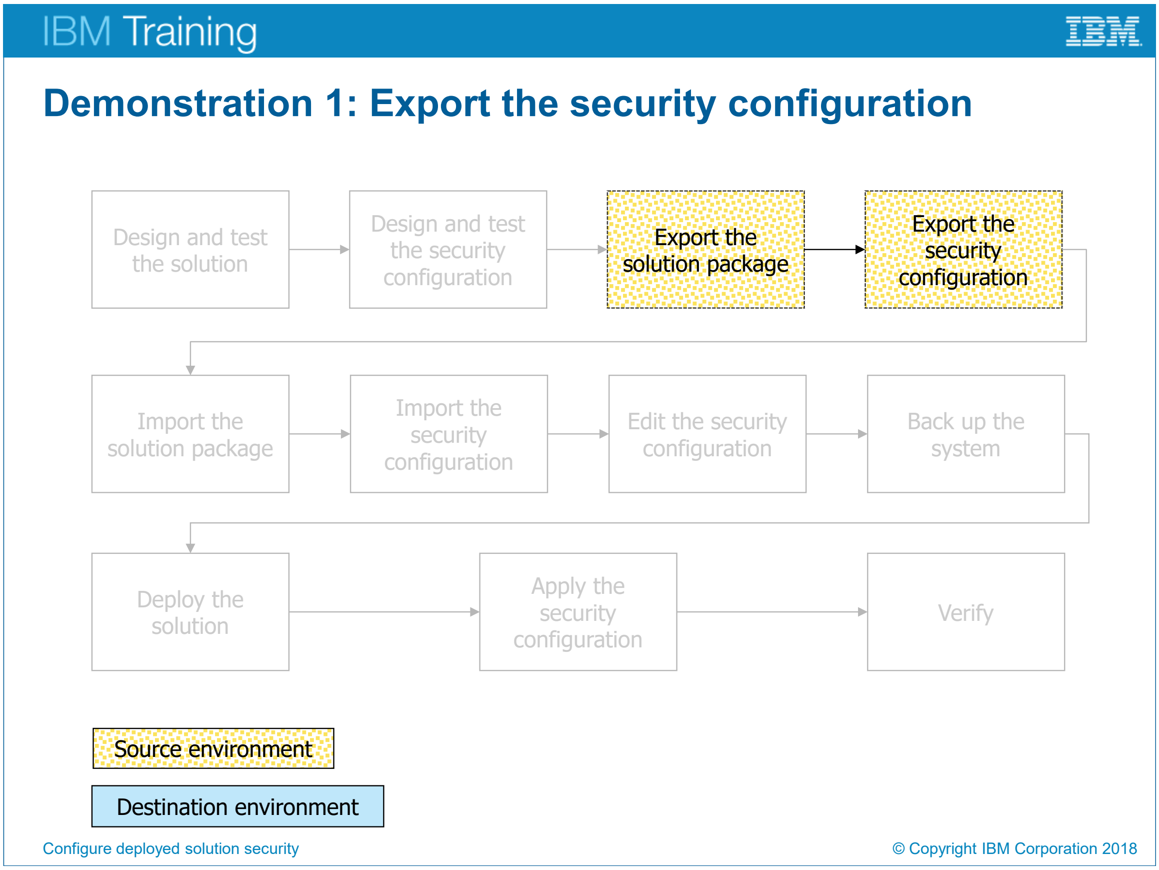
Folder structure and inheritance

The graphic shows the folder hierarchy in a deployed solution.

The deployed case type folder is the source of the security for deployed case types. IBM Case Manager uses the inheritance model with the folder structure to provide access.

In Administration Console for Content Platform Engine, you can expand the target object store folders to see this structure.

Ensure that you give Solution Administrators full control from the deployed solution folder.



IBM Training

Demonstration 1: Export the security configuration

Design and test the solution

Design and test the security configuration

Export the solution package

Export the security configuration

Import the solution package

Import the security configuration

Edit the security configuration

Back up the system

Deploy the solution

Apply the security configuration

Verify

Source environment

Destination environment

Configure deployed solution security

© Copyright IBM Corporation 2018

Demonstration 1: Export the security configuration

The demonstrations in this unit run through the entire process of moving, deploying, and testing the solution in a new environment. You designed the solution and security manifest in previous units. This demonstration focuses on exporting the solution package and the solution configuration manifest.

Demonstration 1: Export the security configuration

Purpose:
Solution development is now at the stage for testing in the user acceptance testing (UAT) environment. Security in the UAT environment is modeled after the production environment. You must export the solution along with the security configuration from the development environment in order to have them ready for import.

Case Admin client URL: **http://vclassbase:9081/navigator/?desktop=icmadmin**

Administrator Username:	**p8admin**
Administrator Password:	**FileNet1**

Task 1. Export the solution package.

1. Use **Filrefox** to log onto **Case Manager administration client** as **p8admin/FileNet1**.
2. Open the **DEV_design** object store.
3. Click **Solutions**.
4. Select the **Medical Visit** solution.
5. Click **Actions** > **Export** > **Solution**.
6. Click **Next**, then click **Finish**.
7. Click **Download and Close**.
8. Select **Save File** and then click **OK**.

Task 2. Export the security configuration.

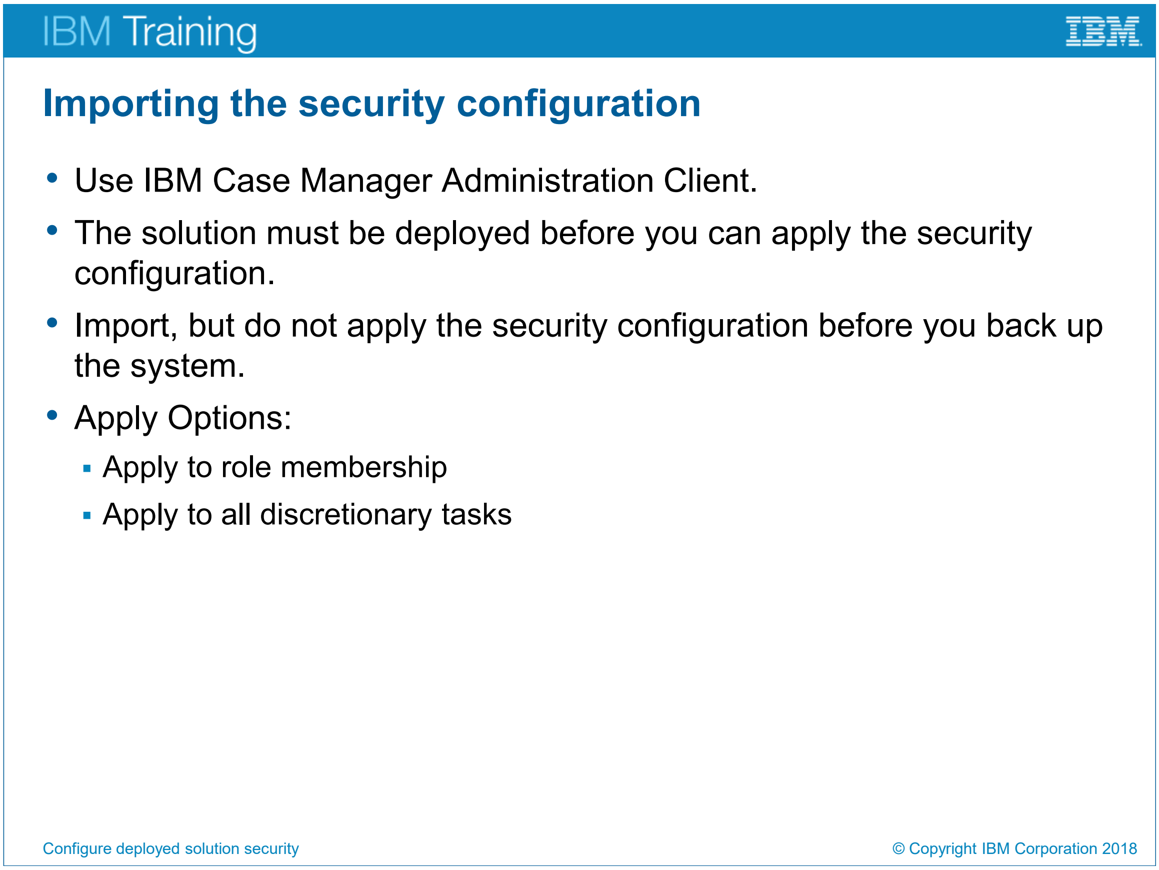
In this procedure, you export the security configuration that is defined for the Medical Visitsolution. You are logged in to IBM Case Manager administration client as an administrator.

1. Select the **Medical Visit** solution.
2. Click **Actions** > **Export** > **Security Configuration**.

   Accept the default name for the Configuration package file name.
3. Under Available manifests: select **MEDSEC,** then click **Next**.
4. On the **Confirm the security configuration to export** page, click **Finish**.
5. Click **Download and Close**.

6. Select **Save File** and then click **OK**.
7. Log out of all applications and close all browsers.

Results:
You exported the solution package and the security configuration for that solution. The two files are in the download folder.



IBM Training

Importing the security configuration

- Use IBM Case Manager Administration Client.
- The solution must be deployed before you can apply the security configuration.
- Import, but do not apply the security configuration before you back up the system.
- Apply Options:
  - Apply to role membership
  - Apply to all discretionary tasks

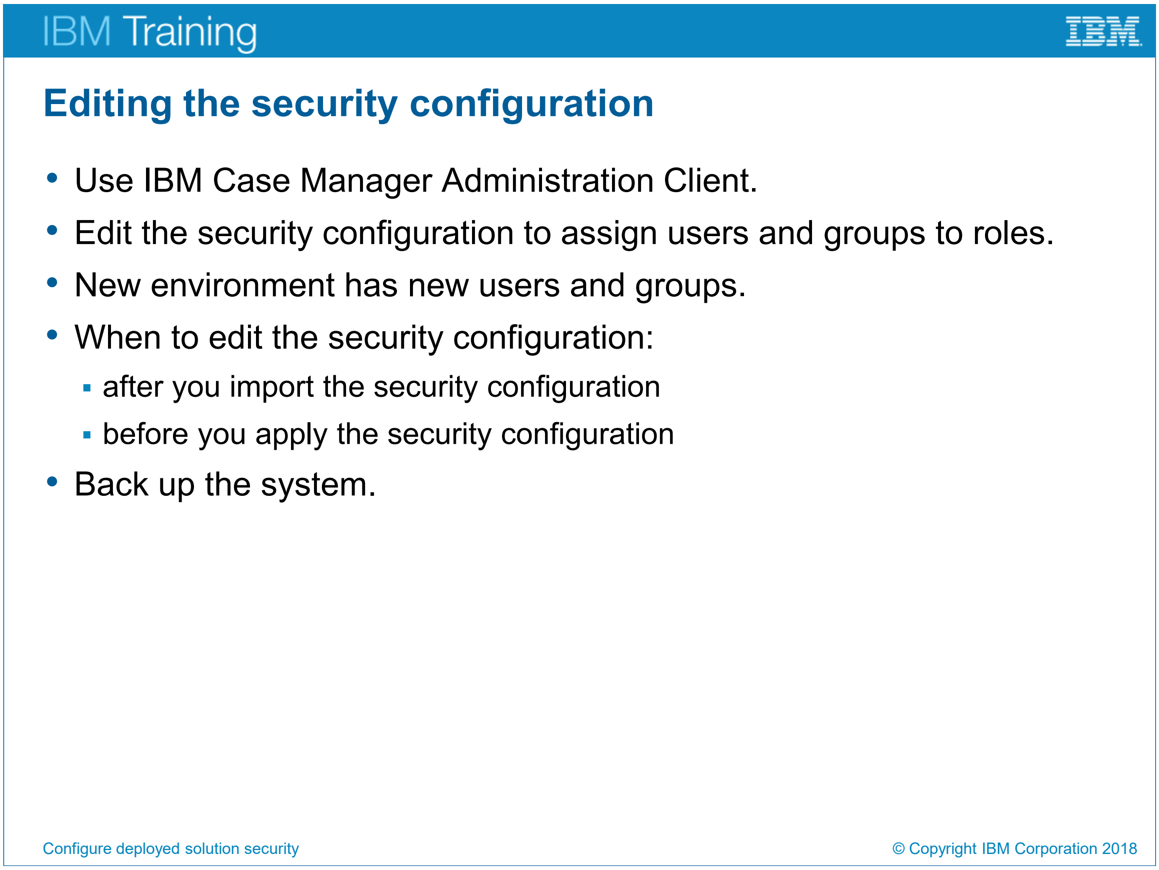
Configure deployed solution security

Importing the security configuration

The solution must be deployed before you can apply the security configuration. When you apply a security configuration, you can select options to apply.

Apply to role membership applies the users and groups that are specified in the security configuration to role membership. Clear this option if you are using Manage Roles in Case Manager Client to assign users to roles.

Apply to all discretionary tasks applies the security configuration to all discretionary tasks. Typically, you apply the security to all discretionary tasks, then configure the exceptions by using Administration Client for Content Platform Engine.



IBM Training

Editing the security configuration

- Use IBM Case Manager Administration Client.
- Edit the security configuration to assign users and groups to roles.
- New environment has new users and groups.
- When to edit the security configuration:
  - after you import the security configuration
  - before you apply the security configuration
- Back up the system.

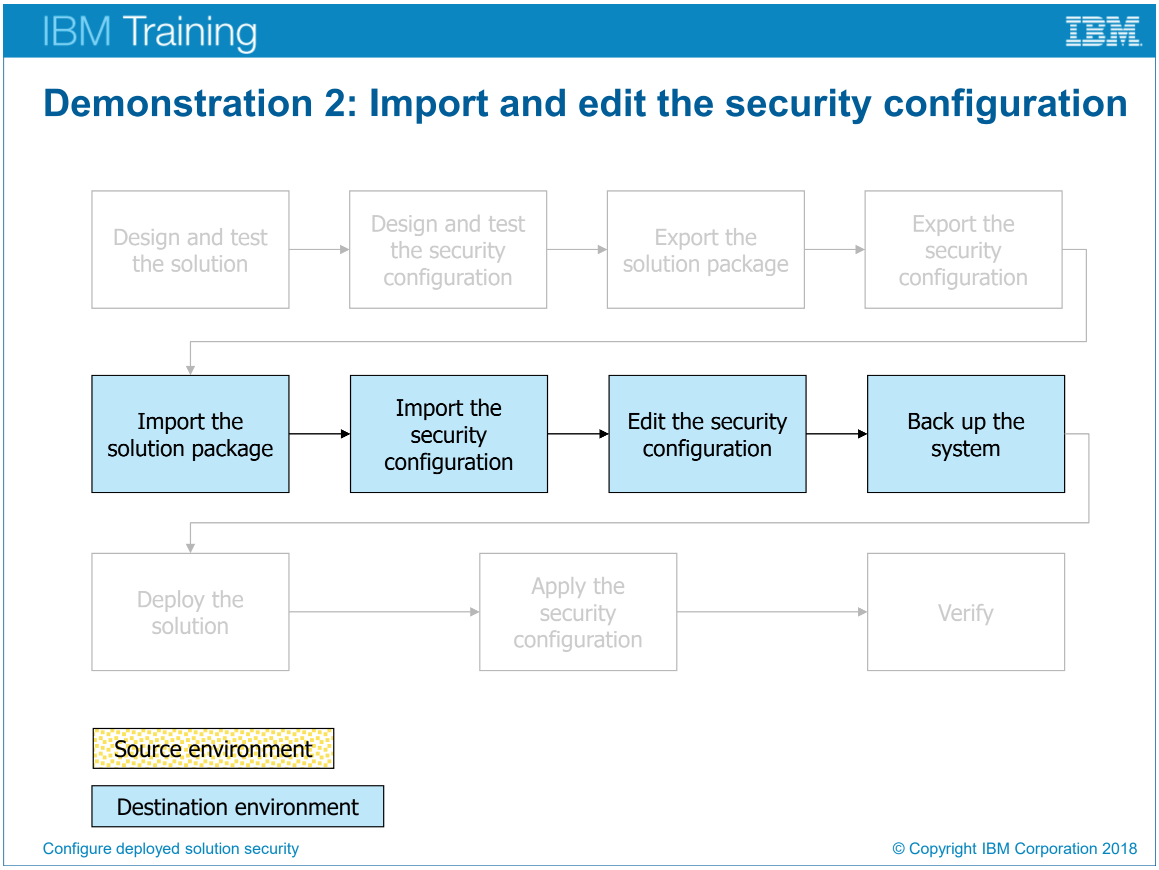
Configure deployed solution security

Editing the security configuration

When you import a security configuration to a new environment, the LDAP users and groups that are assigned to roles must be modified.

You must map users and groups from the new environment to the roles.

After you edit the security configuration, you have done as much work as possible before you deploy the solution. This is a good time to back up the system. If the solution deployment fails for any reason, or you need to undo the solution deployment, having the system backed up just prior to deployment is a good strategy for recovery. If you need to recover the system from the backup, you have minimized the amount of work that must be redone.



IBM Training

Demonstration 2: Import and edit the security configuration

Design and test the solution → Design and test the security configuration → Export the solution package → Export the security configuration

Import the solution package → Import the security configuration → Edit the security configuration → Back up the system

Deploy the solution → Apply the security configuration → Verify

Source environment

Destination environment

Configure deployed solution security

© Copyright IBM Corporation 2018

Demonstration 2: Import and edit the security configuration

The second demonstration requires that the previous demonstration was completed successfully. You have created a solution package and a security configuration package. In this demonstration, you import these packages to the new environment and then edit the security configuration to assign users and groups from the new environment to the solution roles. If possible, you can back up the system before deployment.

Demonstration 2: Import and edit the security configuration

Purpose:
You are transferring a solution from a development environment to a testing environment. After you import the solution and the security configuration, you must edit the security configuration to add users and groups to roles. You are going to edit the security configuration without applying it so that you can back up the system prior to deploying the solution. The UAT environment is already started.

Case Admin client URL: **http://vclassbase:9082/UAT_ICN/?desktop=icmadmin**

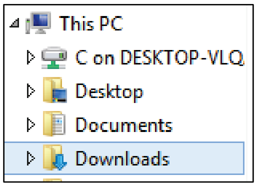
Administrator Username: **p8admin**

AdministratorPassword: **FileNet1**

You are now using the **UAT Case Manager administrator client.**

Task 1. Import the solution.

1. Start **Firefox**.
2. On the Home page, click the **UAT Case Admin** link and log on to **UAT IBM Case Manager administration client** as **p8admin/FileNet1**.
3. Open the **UAT_staging** object store.
4. Right-click **Solutions** > **Import Solution** > **From Solution Package**.
5. Click **Browse** to and then browse to **This PC** > **Downloads**.



6. Select **Medical_Visit_solution.zip** and then click **Open**, then click **Next**.
7. Review the solution package to import, then click **Next**.
8. Confirm that the **Target Name** is **UAT_staging**, then click **Finish**.
9. Wait for the import to complete, then click **Close**.

Task 2. Import the security configuration.

You are logged in to the Case Manager administration client (UAT).

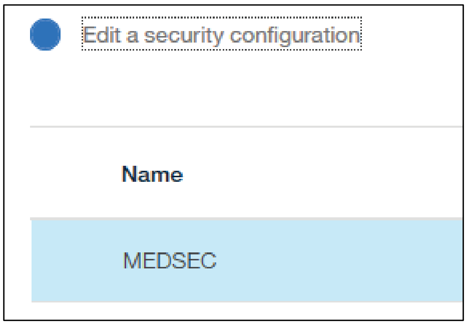
1. Select **UAT_staging** > **Solutions** > **Medical Visit**.
2. Click **Import** > **Import Security Configuration**.

3. Browse to and select **This PC** > **Downloads** > **Medical_Visit_securityManifest.zip.**
4. Click **Open**.
5. Click **Next**.
6. Verify the selected security configuration information:
   - **Solution name: Medical Visit**
   - **IBM Case Manager Version for solution: 5.3.2.0**
   - **Selected configurations: MEDSEC**
7. Click **Finish**.
8. Click **Close**.

Task 3. Edit the security configuration.

In this task, you edit the security configuration prior to deploying the solution. You are already logged on to IBM Case Manager administration client (UAT).

1. Select **UAT_staging** > **Solutions** > **Medical Visit**.
2. Click **Actions** > **Manage** > **Security Configuration**.
3. Select **Edit a security configuration**.
4. Select the **MEDSEC** security configuration.



● Edit a security configuration

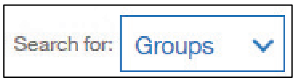
Name
MEDSEC

You might need to scroll down to see MEDSEC.

5. Click **Next**.
6. Click **Next** until you get to the **Associate users and groups with roles** page.

Task 4. Associate users and groups with roles.

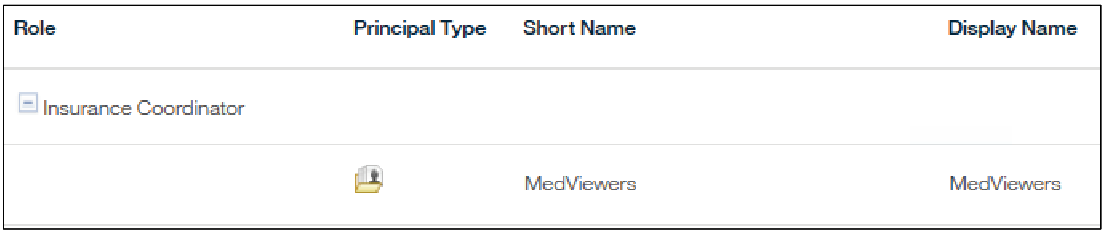
1. On the **Associate users and groups with roles** page, select **Addington**, then click **Remove**.
2. Remove **Sue**, **Cody**, and **Fred**.
3. Select the **Insurance Coordinator** role, then click **Add**.
4. Select **Groups** from the **Search for** menu.



Search for: Groups

5. Search for and then select **MedViewers**.
6. Add **MedViewers** to the **Selected** list. Verify the role in the bottom right: **Insurance Coordinator**, then click **Add**.
7. Expand the **Insurance Coordinator** role.

   The results appear as follows:



Role	Principal Type	Short Name	Display Name
⊟ Insurance Coordinator			
	👥	MedViewers	MedViewers

8. For each of the remaining roles, add the indicated group, then click **Next**:

   - **Nurse: MedWorkers**
   - **Receptionist: MedInitiators**
   - **Physician: MedAdmins**

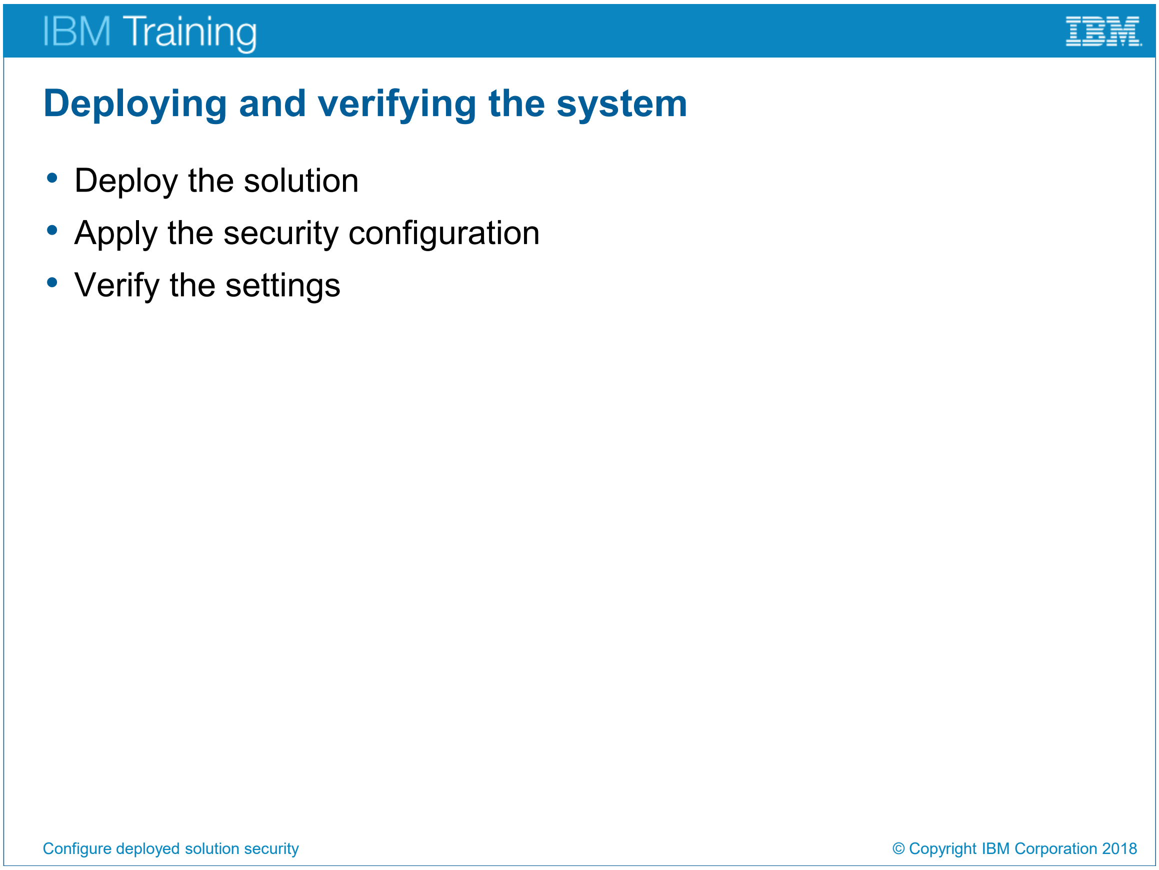
   If you cannot see the Add button, use the scroll bar on the right to move the window up until the menu bar is visible.

   Remember to select Groups before you search.

   Ensure that each of the four roles are assigned to the appropriate group.
9. Click **Save**, then click **Cancel**.
10. Log out of all applications and close all windows.

    This is the point at which you back up the target environment. You do not need to practice backing up your student system.

Results:
You exported a security configuration package file to a new environment. You edited the security configuration.



IBM Training

Deploying and verifying the system

- Deploy the solution
- Apply the security configuration
- Verify the settings

Configure deployed solution security

© Copyright IBM Corporation 2018

Deploying and verifying the system

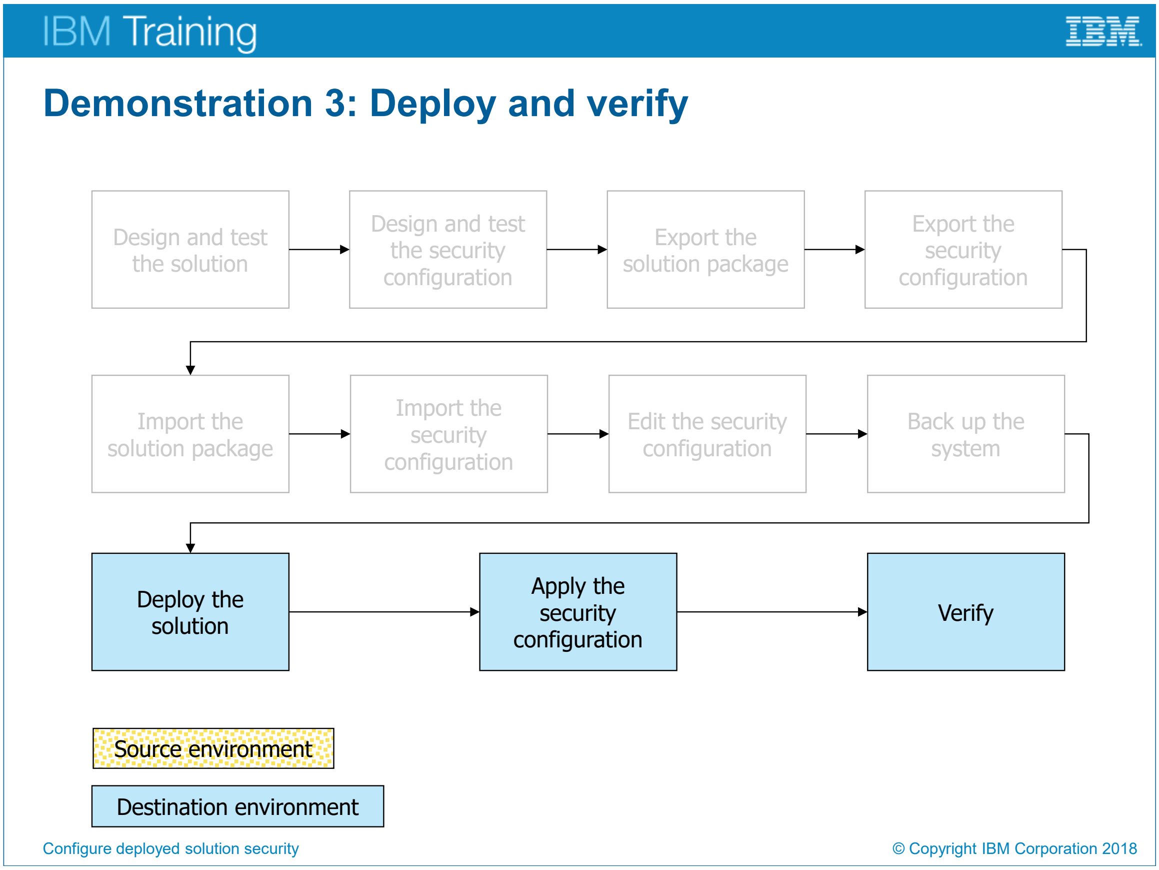
Until this point, you have used Case Manager Builder to deploy and test solutions in the development environment. Case Manager Builder is not installed in non-development environments. In a non-development environment, you must use the Case Manager administration client to deploy the solution.

The solution must be deployed before you can apply the security configuration. If you have already imported and edited the security configuration, you can quickly move through the wizard and apply it to the solution.

After you apply the security configuration, thoroughly test the solution security settings.

Verify the following conditions:

- All roles have correct permissions.
- All roles can complete all of their operations without errors.
- All users belong to the correct groups.
- All groups are assigned correctly to the roles.



IBM Training

Demonstration 3: Deploy and verify

Design and test the solution → Design and test the security configuration → Export the solution package → Export the security configuration

Import the solution package → Import the security configuration → Edit the security configuration → Back up the system

Deploy the solution → Apply the security configuration → Verify

Source environment

Destination environment

Configure deployed solution security

© Copyright IBM Corporation 2018

Demonstration 3: Deploy and verify

When you import a security configuration to a new environment, the users and groups that are assigned to roles must be modified. You must map users and groups from the new environment to the roles.

Demonstration 3: Deploy and verify

Purpose:
You have imported a solution and a security configuration into the UAT testing environment. You backed up the system. Now you are going to deploy the solution and apply the security configuration.

Case Admin client URL: **http://vclassbase:9082/UAT_ICN/?desktop=icmadmin**

Administrator Username:	**p8admin**
AdministratorPassword:	**FileNet1**

Task 1. Deploy the solution.

1. Open **Firefox** and then click the **UAT Case Admin** link. Log on to **Case Manager administration client (UAT)** as **p8admin/FileNet1**.
2. Open the **UAT_staging** object store.
3. Expand **Solutions**.
4. Right-click **Solutions** > **Medical Visit** and then click **Deploy**.
5. In **Select the target object environment**, ensure that **UAT_target_env** is selected.
6. Click **Finish**. Wait for the operation to complete.
7. Click **Close**, or optionally **View Log**.

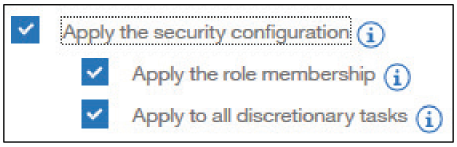
Task 2. Apply the security configuration.

You have already assigned groups to the roles. The only thing left to do is to get to the end of the wizard and then apply the security configuration. You are still logged on to Case Manager administration client (UAT). You are viewing the Solutions tab of the UAT_Staging object store.

1. Click **UAT_staging** > **Solutions**.
2. Select the **Medical Visit** solution.
3. Click **Actions** > **Manage** > **Security Configuration**.
4. Select **Edit a security configuration**, then select the **MEDSEC** security configuration, and then click **Next**.
5. Click **Next** until you get to the **Apply the security configuration** page.
6. Select the **Apply the security configuration** check box.

7. Verify that the other two boxes are also checked.

   The results appear as follows:



☑ Apply the security configuration ⓘ
- ☑ Apply the role membership ⓘ
- ☑ Apply to all discretionary tasks ⓘ

8. Click **Apply** and then wait for the operation to complete.
9. Verify that you see a success message.
10. Click **Close**, or optionally **View Log**.
11. Log out of **IBM Case Manager administration client** and then close **Firefox**.

Task 3. Test solution security in the UAT environment.

1. In **Firefox**, open the Home page, then click the **UAT Case Client** link.
2. Log in to **IBM Case Manager Client for UAT** as **Roberta/FileNet1**, confirm the following settings, then log out:

   - Role: **Receptionist**.
   - **Add Case** button state: active.

   If you experienced unexpected results, skip to task 4, then repeat this task.
3. Log in to **IBM Case Manager Client for UAT** as **Peter/FileNet1**, confirm the following settings, then log out:

   - **Role**: **Physician**.
   - **Add Case** button state: inactive.
4. Log in to **IBM Case Manager Client for UAT** as **Clara**, confirm the role: **Insurance Coordinator**, then log out.
5. Log in to **IBM Case Manager Client for UAT** as **Oscar**, confirm the role: **Nurse**, then log out.

   If all of the accounts worked as expected, skip to task 6.

Task 4. Clear the browser cache (optional).

Complete this task if no solution or role is visible after you log into Case Manager Client. Otherwise, proceed to task 6.

1. Log out of **IBM Case Manager Client for UAT**.
2. Open the Firefox settings menu ☰.
3. Click **History** 🕘 History.
4. Click **Clear Recent History** near the top.
5. Click **Clear Now**.

6. Try logging in to **Case Manager Client** as **Roberta/FileNet1** again.

   If you are able to see the solution and the correct role, return to task 4. Otherwise, proceed to task 5.

Task 5. Restart WebSphere (optional).

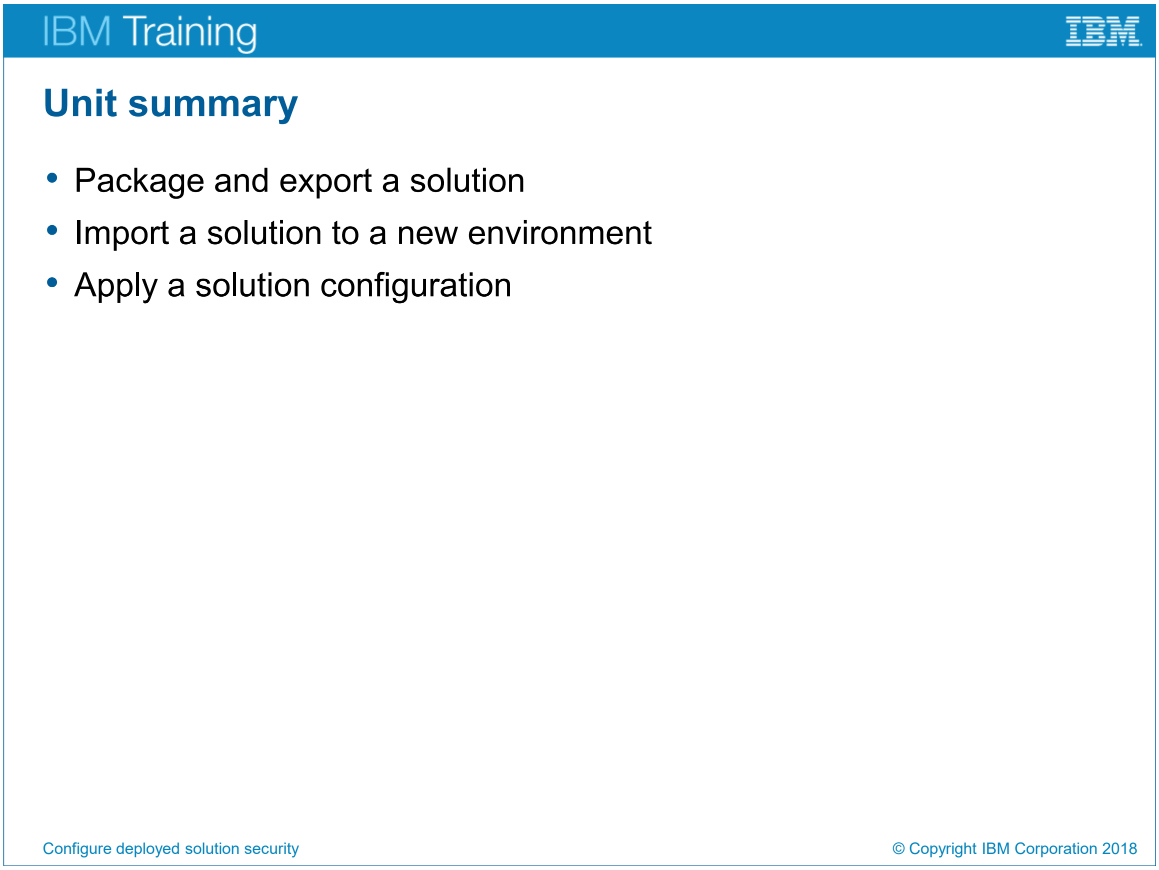
Complete this task only if clearing the browser cache did not fix the login issue. Wait for each program to complete before running the next.

1. Open the **WebSphere Admin** folder on your desktop.
2. Run **_3 Stop ICNserver.bat** as administrator.
3. Run **_4 Stop server1.bat** as administrator.
4. Open **Start** > **Services**.
5. Restart **IBM WebSphere Application Server V9.0 – UATNode01**.
6. Run **_1 Start server1.bat** as administrator.
7. Run **_2 Start ICNserver.bat** as administrator.
8. If the problem persists, restart your student system and then repeat steps 1, 4, 5, 6, and 7 from this task.

Task 6. Process a test case.

1. Log in to **IBM Case Manager Client for UAT** as **Roberta/FileNet1**.
2. Add an **Office Visit** case.
3. Enter the client name: `UAT_test`.
4. On the **Work** tab, complete the **Sign In** step as **Roberta**, then log out.
5. Log in as **Clara/FileNet1** to complete the **Check Insurance** step, then log out.
6. Log in as **Roberta/FileNet1** to complete the **Collect Copay** step, then log out.
7. Log in as **Oscar/FileNet1** to complete the **Get Vitals** step, then log out.
8. Log in as **Peter/FileNet1** to complete the **Consultation** step, then log out.
9. Log out of all applications and close all browsers.

Results:
You deployed a solution in a new environment. You applied the security configuration and tested the solution to ensure that security settings were properly applied.



IBM Training

Unit summary

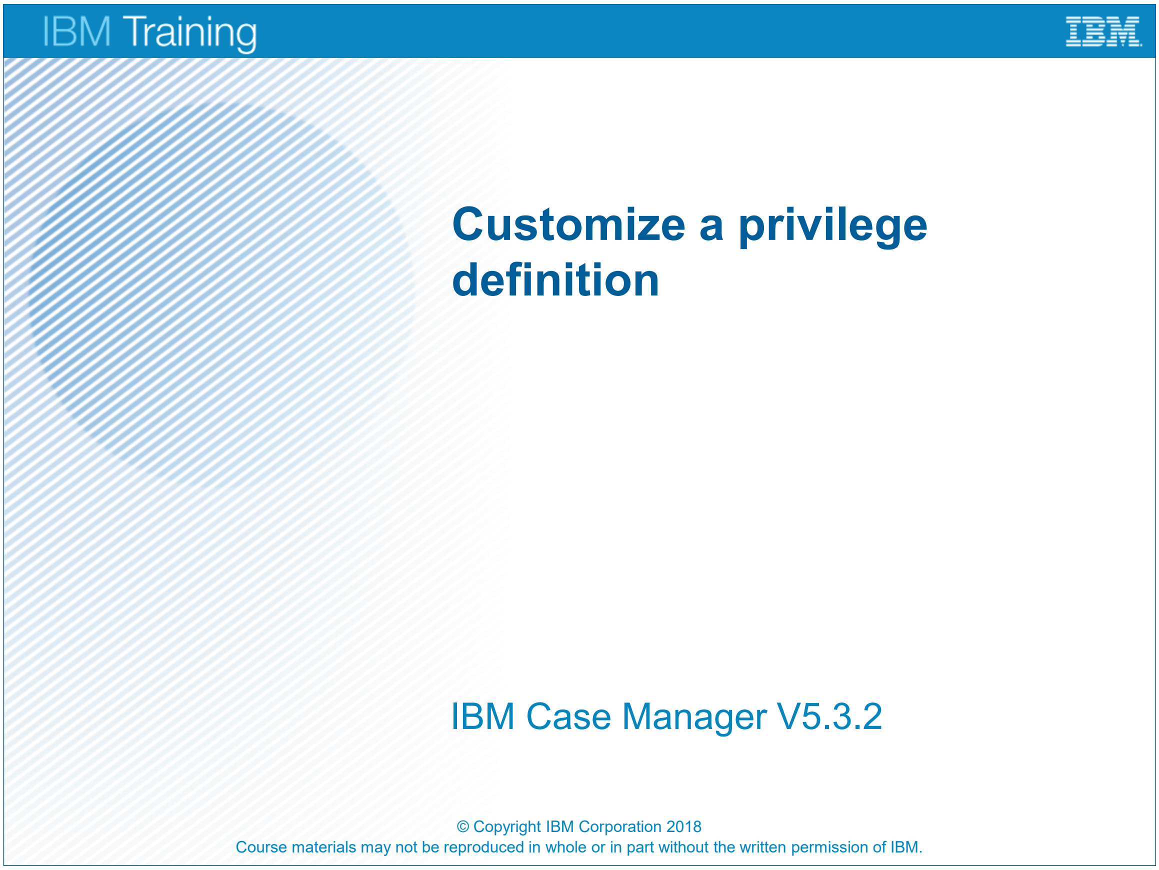
- Package and export a solution
- Import a solution to a new environment
- Apply a solution configuration

Configure deployed solution security

© Copyright IBM Corporation 2018

Unit summary

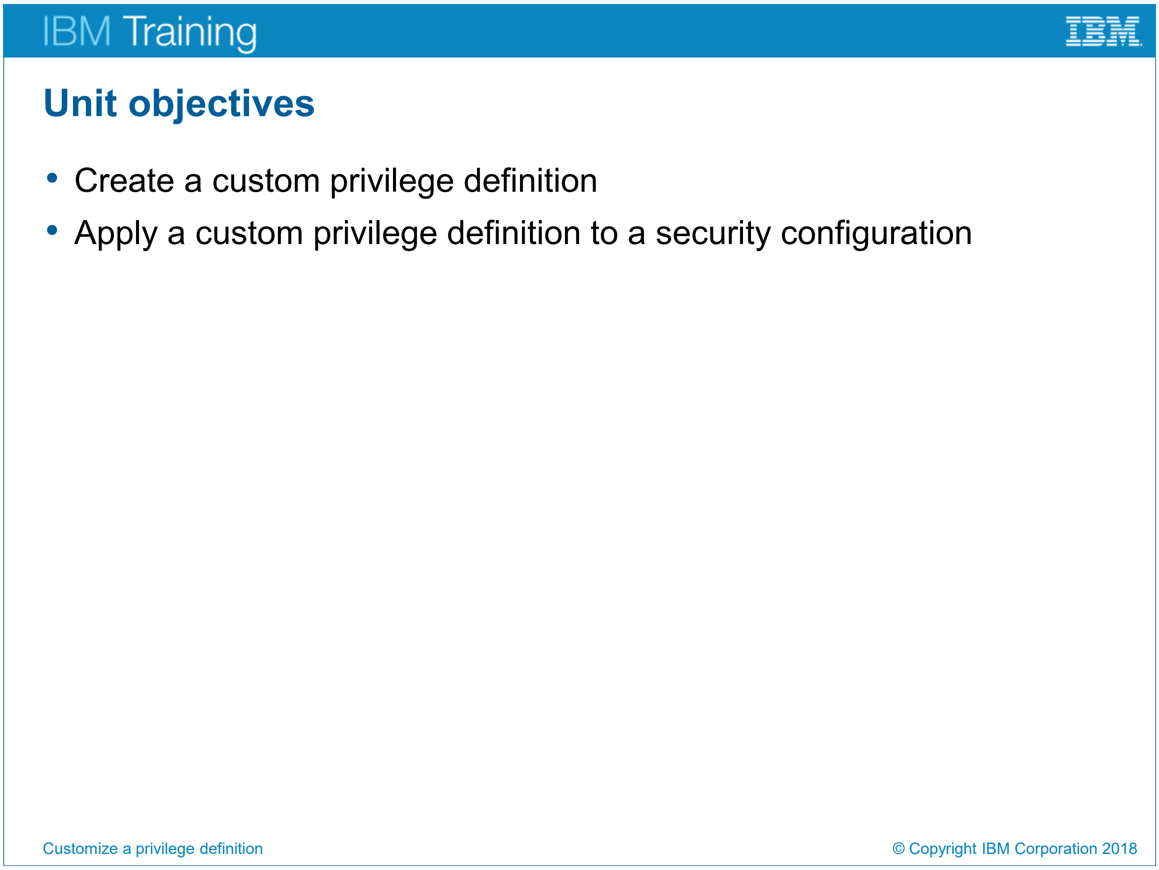
Unit 7 Customize a privilege definition



IBM Training

Customize a privilege definition

IBM Case Manager V5.3.2



IBM Training

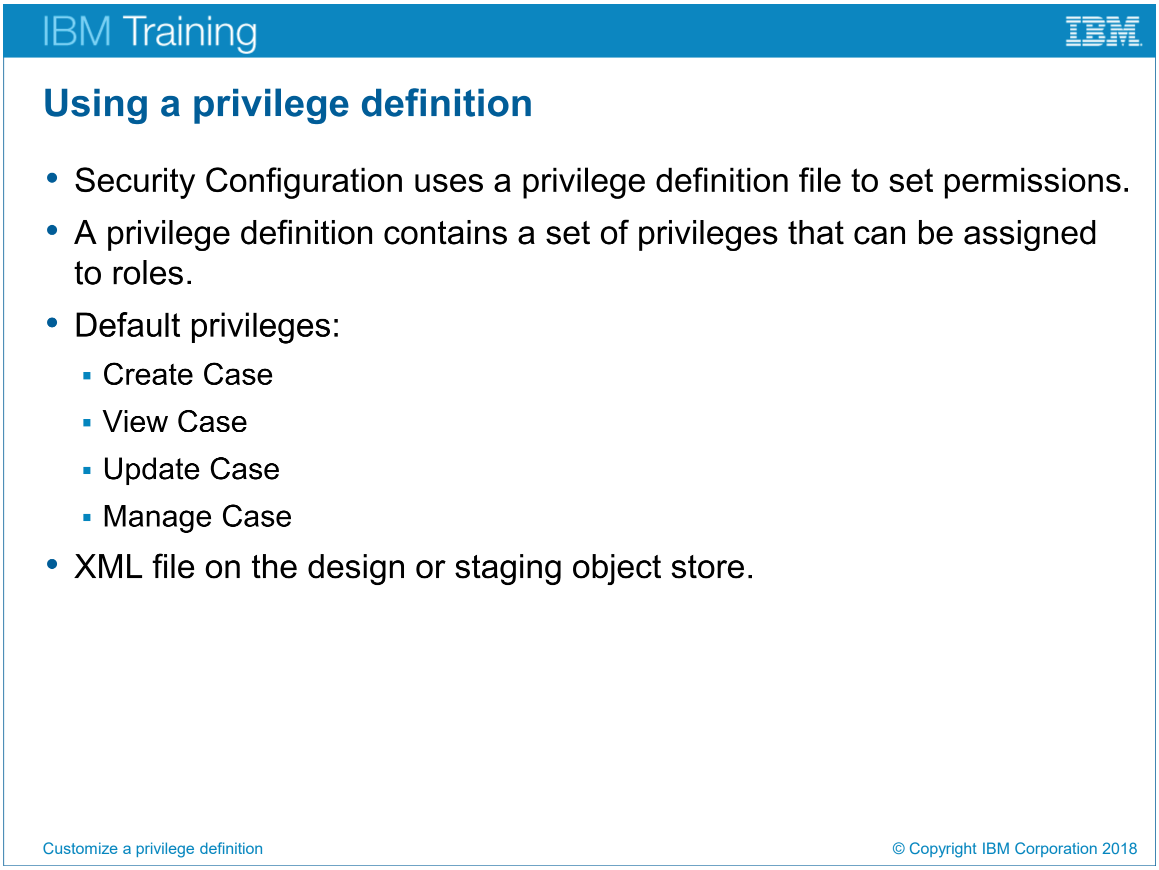
Unit objectives

- Create a custom privilege definition
- Apply a custom privilege definition to a security configuration

Customize a privilege definition

© Copyright IBM Corporation 2018

Unit objectives



IBM Training

Using a privilege definition

- Security Configuration uses a privilege definition file to set permissions.
- A privilege definition contains a set of privileges that can be assigned to roles.
- Default privileges:
  - Create Case
  - View Case
  - Update Case
  - Manage Case
- XML file on the design or staging object store.

Customize a privilege definition

© Copyright IBM Corporation 2018

Using a privilege definition

The Security Configuration includes predefined privilege sets that work for most applications. However, some situations require that you customize privileges. You can edit the privilege definition to provide customized privileges for your roles.

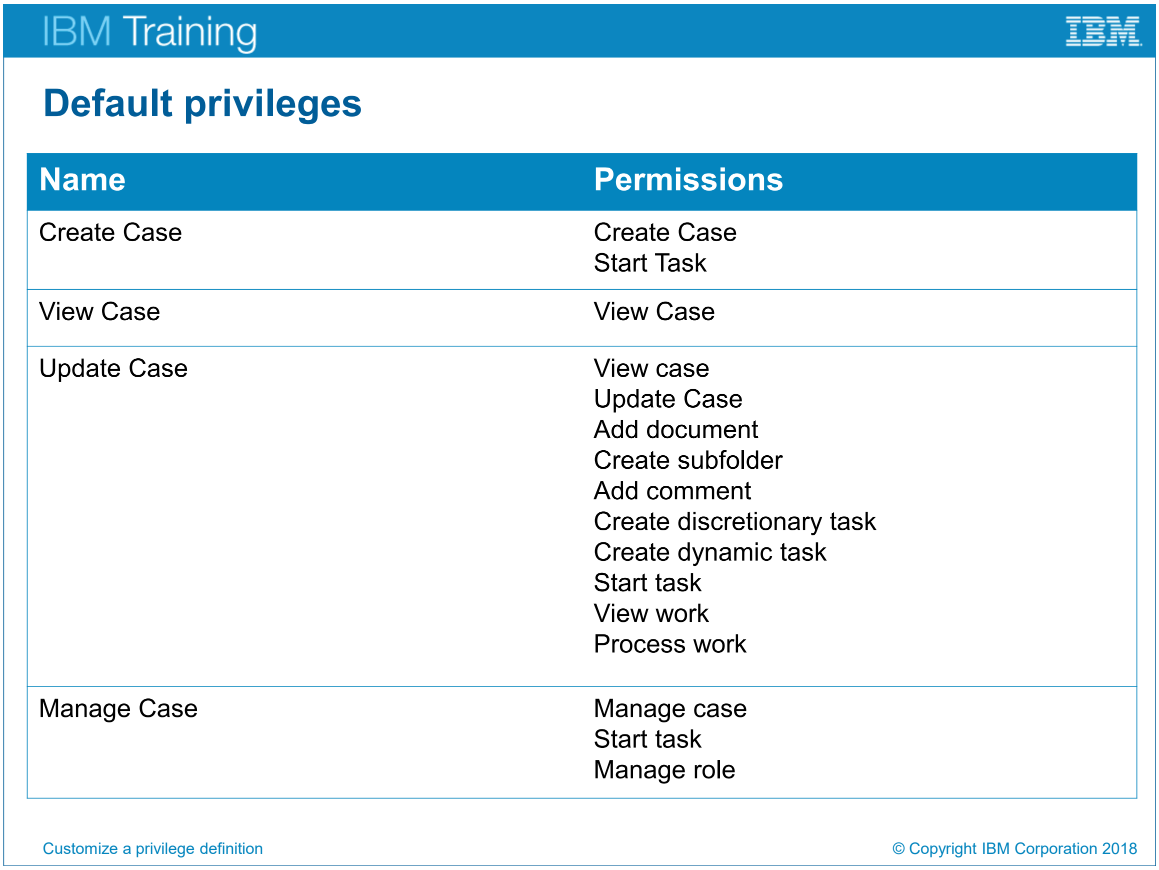
A privilege definition is a set of privileges that can be assigned to roles. Privilege definitions are assigned to roles with the Security Configuration wizard.

The privilege definition has default privileges for creating, viewing, updating, and managing a case.

The privilege definition file is an XML file that defines the privilege definitions that are used in a solution.

You can find the security definition file on the design or staging object store:

- Location: object_store\Root Folder\IBM Case Manager\Security Configurations\Privilege Definitions folder.
- File name: ICMPrivilegeDefinition.xml.



IBM Training

Default privileges

Name	Permissions
Create Case	Create Case Start Task
View Case	View Case
Update Case	View case Update Case Add document Create subfolder Add comment Create discretionary task Create dynamic task Start task View work Process work
Manage Case	Manage case Start task Manage role

Customize a privilege definition

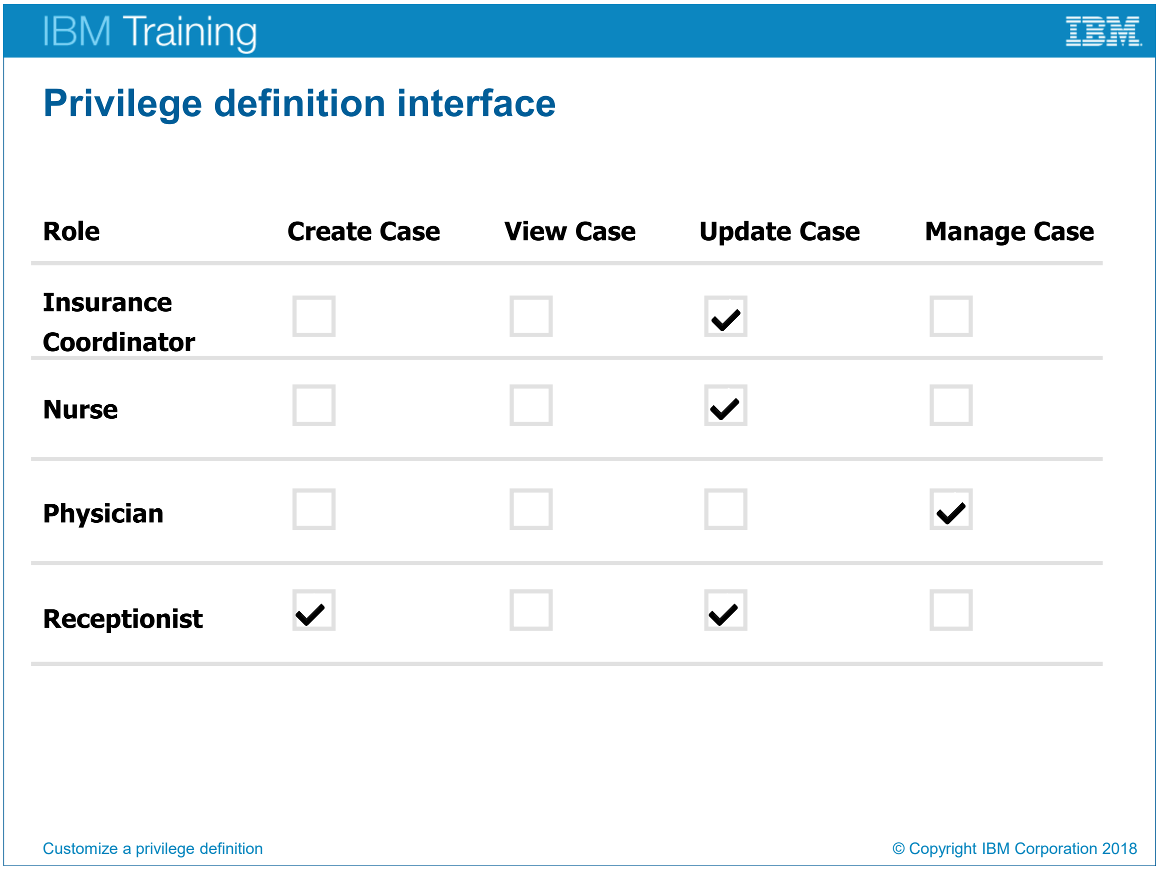
© Copyright IBM Corporation 2018

Default privileges

Each privilege consists of one or more permissions that are defined in a privilege definition file.

The default privileges work in most applications. However, some applications might require a specialized set of permissions that are not available in the default privilege definition file.

For example, you might want someone with View Case privileges to be able to add case comments. By default, the View Case privilege does not include permission to add comments. You can customize the privilege definition file to allow users with View Case access to include this permission.



IBM Training

Privilege definition interface

Role	Create Case	View Case	Update Case	Manage Case
Insurance Coordinator	□	□	☑	□
Nurse	□	□	☑	□
Physician	□	□	□	☑
Receptionist	☑	□	☑	□

Customize a privilege definition

© Copyright IBM Corporation 2018

Privilege definition interface

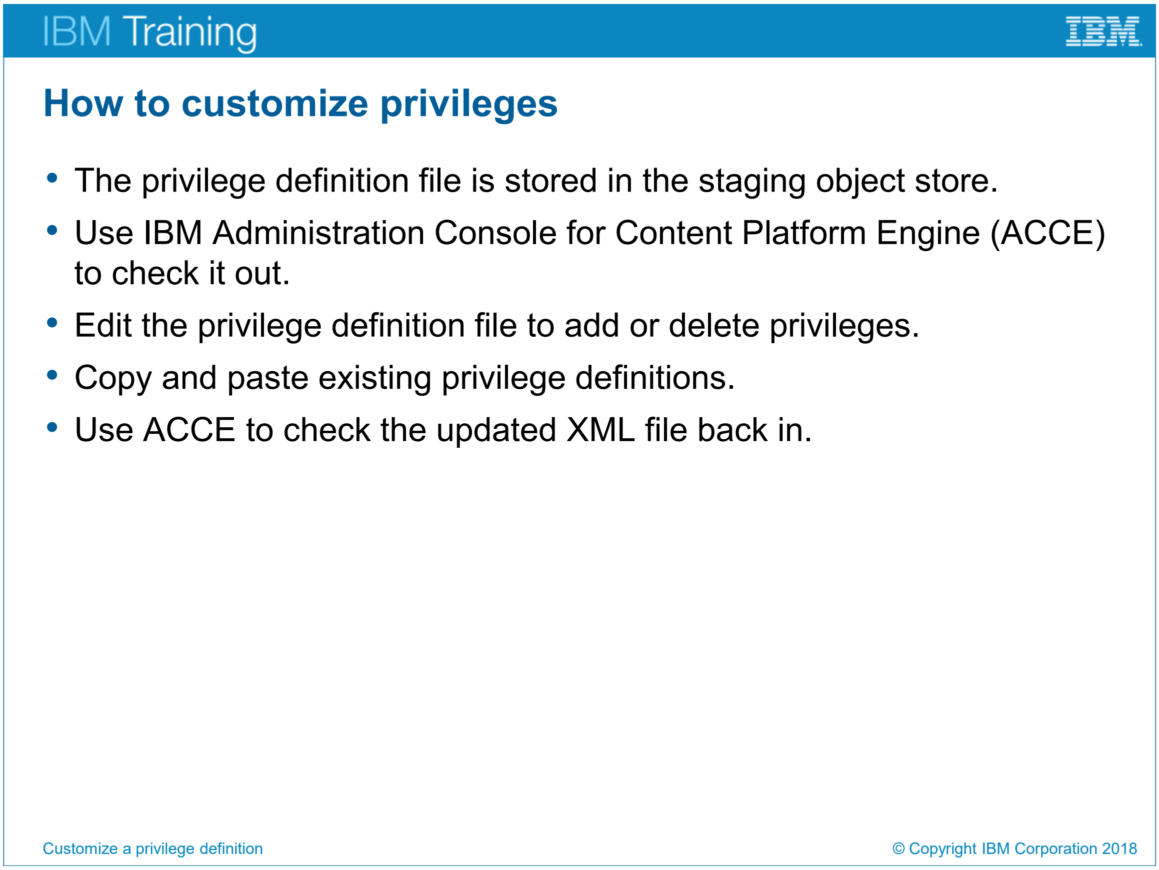
The graphic shows default privileges definition in the Security Configuration wizard. The privileges include:

- Create Case
- View Case
- Update Case
- Manage Case

For more information about specific permissions, refer to the Knowledge Center topic:

IBM Case Manager V5.2.1 > Security > Configuring Security for IBM Case Manager solutions > Privilege definition reference

https://www.ibm.com/support/knowledgecenter/SSCTJ4_5.3.2/com.ibm.casemgmt.design.doc/acmdc090.htm



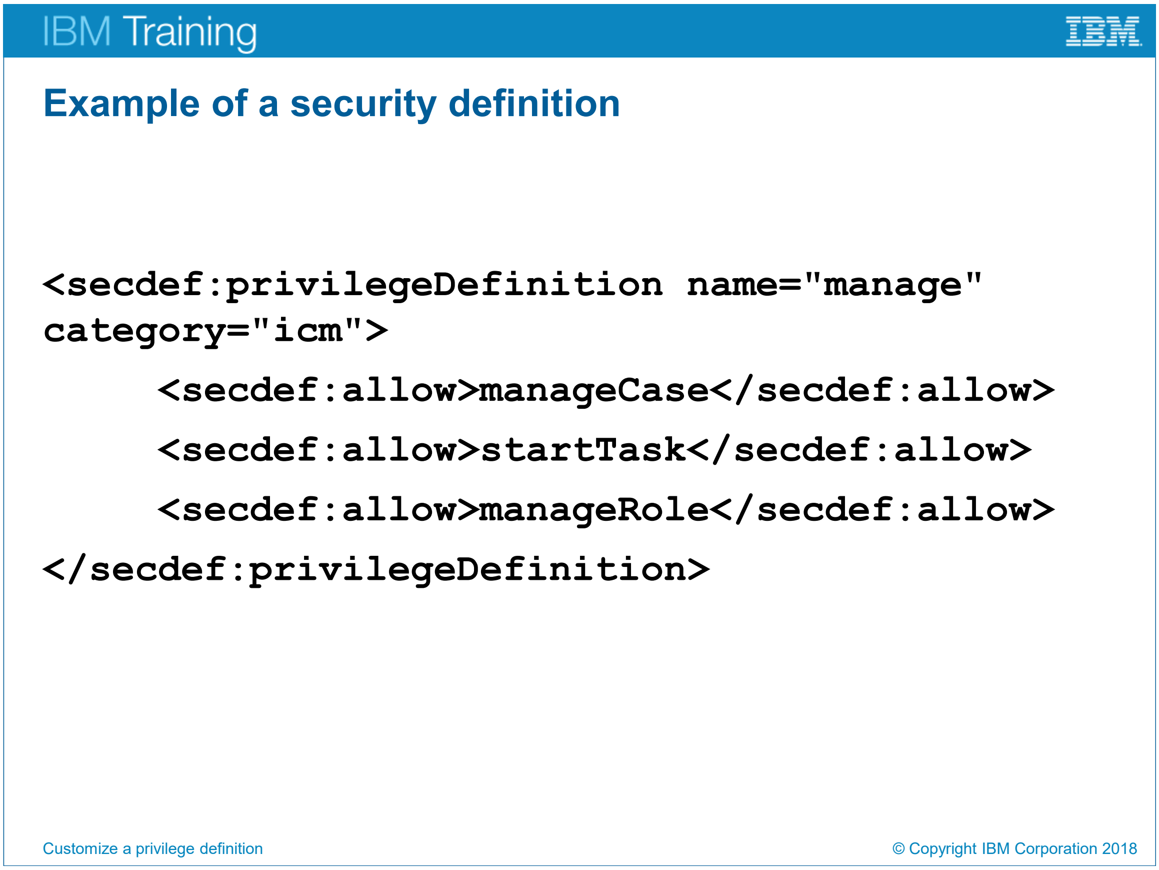
IBM Training

How to customize privileges

- The privilege definition file is stored in the staging object store.
- Use IBM Administration Console for Content Platform Engine (ACCE) to check it out.
- Edit the privilege definition file to add or delete privileges.
- Copy and paste existing privilege definitions.
- Use ACCE to check the updated XML file back in.

Customize a privilege definition

How to customize privileges



IBM Training

Example of a security definition

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

Customize a privilege definition

Example of a security definition

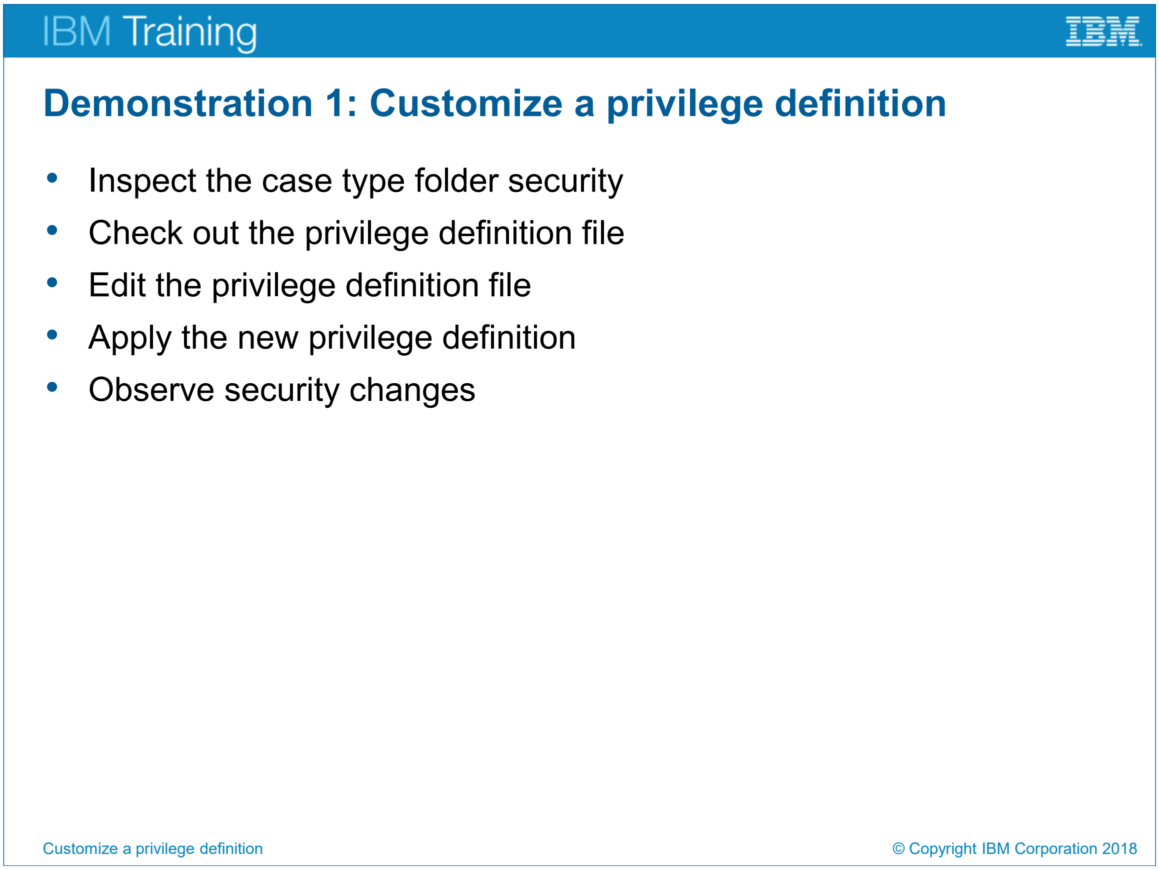
Read the comments in the security definition file to help you edit the file.

In this example, the privilege definition name is "manage." Privileges include the category "icm."

The manage privilege definition includes the following permissions:

- manageCase
- startTask
- manageRole

You can add a new security definition by adding a <secdef:privilegeDefinition> element with appropriate <secdef:allow> elements. The easiest way to do this is to copy an existing security definition and renaming it.



IBM Training

Demonstration 1: Customize a privilege definition

- Inspect the case type folder security
- Check out the privilege definition file
- Edit the privilege definition file
- Apply the new privilege definition
- Observe security changes

Customize a privilege definition

Demonstration 1: Customize a privilege definition

Demonstration 1: Customize a privilege definition

Purpose:
Insurance coordinators currently have permission to update cases, add comments, folders, documents to the case. You need to remove some of these permissions by creating a custom privilege definition that allows them to update cases and processes, but not add comments, folders, or documents to the case.

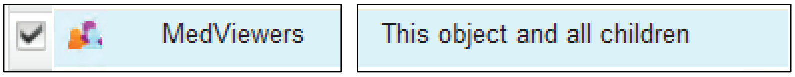
Case Admin client URL: **http://vclassbase:9081/navigator/?desktop=icmadmin**

Administrator account:	**p8admin/FileNet1**
Receptionist account:	**Roberta/FileNet1**
Insurance account:	**Clara/FileNet1**
Nurse account:	**Oscar/FileNet1**
Physician account:	**Peter/FileNet1**

Task 1. Inspect the case type folder security.

The deployed case type folder object is a parent object for case folder security inheritance. Changes to this folder affect all case folders of this case type.

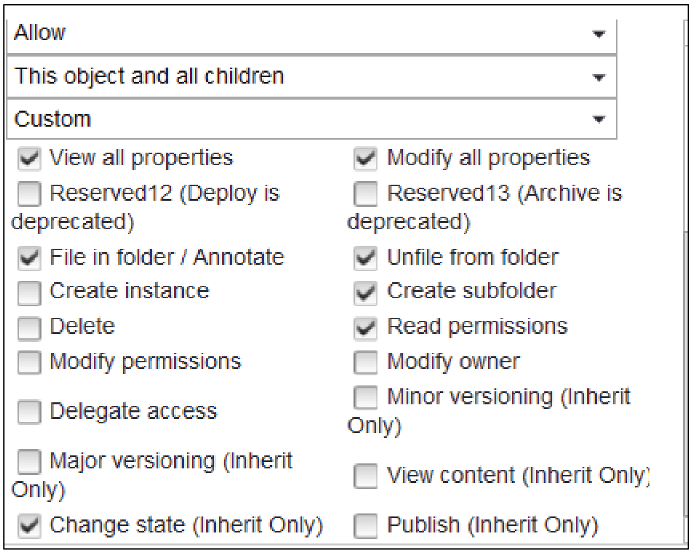
1. In **Firefox**, click the **ACCE** link on the home page.
2. Log in to **Administration Console for Content Platform Engine** as **p8admin/FileNet1**.
3. Open the **UAT_target** object store.
4. Navigate to **Browse** > **Root Folder** > **IBM Case Manager** > **Solution Deployments** > **Medical Visit** > **Case Types**.
5. Select **MED_OfficeVisit**.
6. Open the **Security** tab.
7. Check the box next to **MedViewers** where the **Apply To** column shows **This Object and All Children.**



☑ MedViewers | This object and all children

8. Click **Edit** to review the permissions on this object.

   The results appear as follows:



Allow ▾

This object and all children ▾

Custom ▾

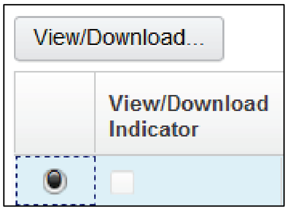
☑ View all properties	☑ Modify all properties
☐ Reserved12 (Deploy is deprecated)	☐ Reserved13 (Archive is deprecated)
☑ File in folder / Annotate	☑ Unfile from folder
☐ Create instance	☑ Create subfolder
☐ Delete	☑ Read permissions
☐ Modify permissions	☐ Modify owner
☐ Delegate access	☐ Minor versioning (Inherit Only)
☐ Major versioning (Inherit Only)	☐ View content (Inherit Only)
☑ Change state (Inherit Only)	☐ Publish (Inherit Only)

9. Verify that the group has the following permissions:
   - **View all properties**
   - **File in folder / Annotate**
   - **Change state (Inherit Only)**
   - **Modify all properties**
   - **Unfile from Folder**
   - **Create subfolder**
   - **Read permissions**
10. Click **Cancel**.
11. Close the **UAT_target** object store tab, but remain logged in Administration Console.

Task 2. Check out the privilege definition.

1. Open the **UAT_staging** object store.
2. Expand **Browse** > **Root Folder** > **IBM Case Manager** > **Security Configurations** > **Privilege Definitions**, and then click **ICM Privilege Definition**.
3. Click **Actions** > **Checkin, checkout, cancel** > **Exclusive Checkout**.

4. On the Exclusive checkout wizard, select the file and then click **View/Download**.



5. Select the **Save File** option, and then click **OK**.
6. Click **Checkout**.
7. Log out of **Administration Console**.

Task 3. Edit the privilege definition.

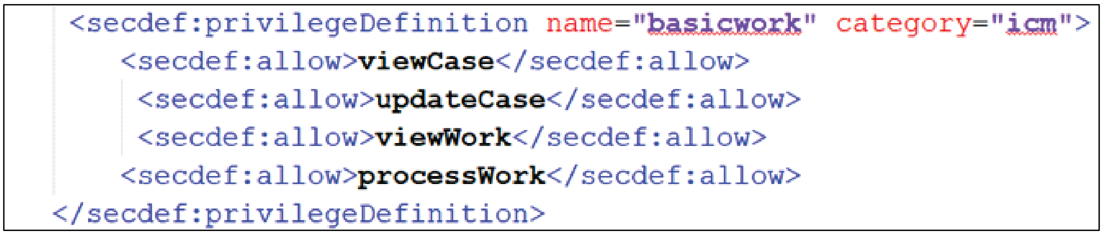
1. In **Firefox**, click the **Downloads** button in the top right ⤓.
2. Right-click **ICMPrivilegeDefinition.xml** and then select **Open Containing Folder**.
3. From the Downloads folder, right-click **ICMPrivilegeDefinition.xml** and then select **Edit with Notepad ++**.
4. Read the instructions in the file for editing information.
5. Create a new privilege definition by copying and pasting the “view” privilege definition:

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

6. In the copied text, replace **“view”** with `"basicwork"`.
7. Type or copy and paste the following permissions into the basicwork privilege definition:

- **<secdef:allow>updateCase</secdef:allow>**
- **<secdef:allow>viewWork</secdef:allow>**
- **<secdef:allow>processWork</secdef:allow>**

The results appear as follows:



```
 <secdef:privilegeDefinition name="basicwork" category="icm">
    <secdef:allow>viewCase</secdef:allow>
     <secdef:allow>updateCase</secdef:allow>
     <secdef:allow>viewWork</secdef:allow>
    <secdef:allow>processWork</secdef:allow>
</secdef:privilegeDefinition>
```

8. Save the file and then close **Notepad ++**.

Task 4. Check in the privilege definition.

1. Log in to **Administration Console for Content Platform Engine** as **p8admin/FileNet1**.
2. Open the **UAT_staging** object store.
3. Expand **Browse** > **Root Folder** > **IBM Case Manager** > **Security Configurations** > **Privilege Definitions**.

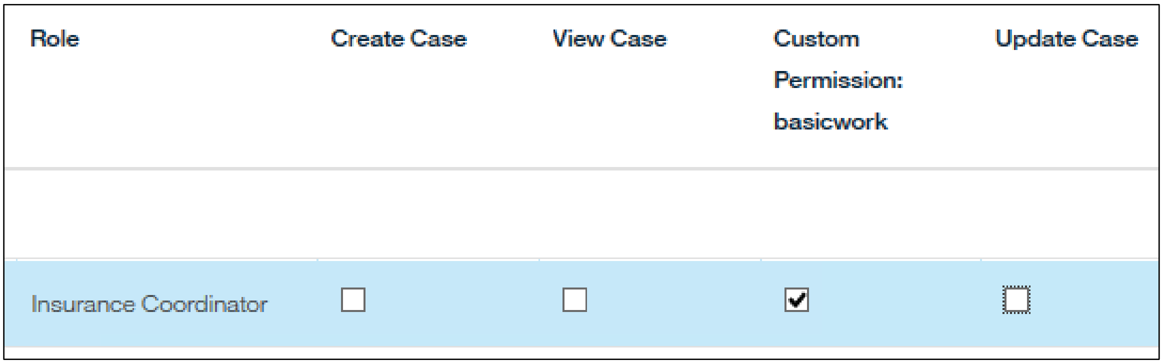
   The file has an indicator showing that it is checked out 🔒.
4. Click **ICM Privilege Definition**.
5. Click **Actions** > **Checkin**, **checkout**, **cancel** > **Checkin,** then click **Add**.
6. In the **Add Content Element** window, click **Browse**.
7. From the **Downloads** folder, select **ICMPrivilegeDefinition.xml**, then click **Add Content**.
8. Click **Check In Major Version**.
9. Log out of **Administration Console for Content Platform Engine**.

Task 5. Apply the security configuration.

1. In **Firefox**, open the Home page, then click the **UAT Case Admin** link to go to the Case Manager Administration Client for the UAT environment and then log on as **p8admin/FileNet1**.
2. Open the **UAT_staging** object store and then navigate to **Solutions**, and then click **Medical Visit** in the main panel.
3. **Click Actions** > **Manage** > **Security Configuration**.
4. Select the **Edit Security Configuration** option, then select **MEDSEC**, then click **Next**.
5. Click **Next** on the **Name the security configuration** page.
6. On the Modify permissions for roles confirm that there is a new permission titled **Custom Permission: basicwork**.

7. For Insurance Coordinator, clear the checkbox for **Update Case** and then place a check mark in the new column, **Custom Permission: basicwork**.

   The results appear as follows:



Role	Create Case	View Case	Custom Permission: basicwork	Update Case
Insurance Coordinator	☐	☐	☑	☐

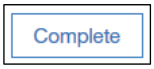
8. Click **Save**, then click **Next** until you get to the **Apply the security configuration** page.
9. Select the **Apply the security configuration** check box, then click **Apply**.
10. Wait for the success message, then log out of **Case Manager Administration Client**.

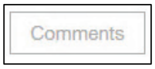
Task 6. Review the case type folder security.

1. In **Firefox**, click the **ACCE** link on the home page.
2. Log in to **Administration Console for Content Platform Engine** as **p8admin/FileNet1**.
3. Open the **UAT_target** object store.
4. Navigate to **Browse** > **Root Folder** > **IBM Case Manager** > **Solution Deployments** > **Medical Visit** > **Case Types**.
5. Select **MED_OfficeVisit**.
6. Open the **Security** tab.
7. Check the box next to **MedViewers** where the **Apply To** column shows **This Object and All Children.**
8. Click **Edit** to review the permissions on this object and then verify that the group has the following permissions:
   - **View all properties**
   - **Modify all properties**
   - **Read permissions**
9. Compare these security settings with the settings that you observed in Task 1.
10. Click Cancel and then log out of **Administration Console for Content Platform Engine**.

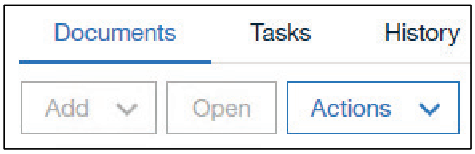
Task 7. Test the security configuration

1. In **Firefox**, open the Home page and then click the **UAT Case Client** link.
2. Log in to **IBM Case Manager for UAT** as **Roberta/FileNet1**, and then add an **Office Visit** case.
3. In the **Client Name** field, type `Warwick`, then click **Add**.
4. Open the **Work** tab.
5. Complete the **Sign In** step, then log out of **IBM Case Manager for UAT**.
6. Log in to **IBM Case Manager for UAT** as **Clara/FileNet1**, open the **Work** tab, and then open the **Check Insurance** step.
7. Verify the following settings:

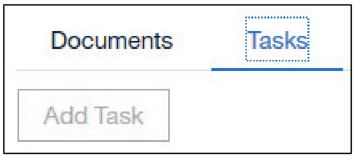
   - The **Complete** button is active .

   - The **Comments** button is inactive .

   - On the Documents tab, the **Add** and **Open** buttons are inactive.

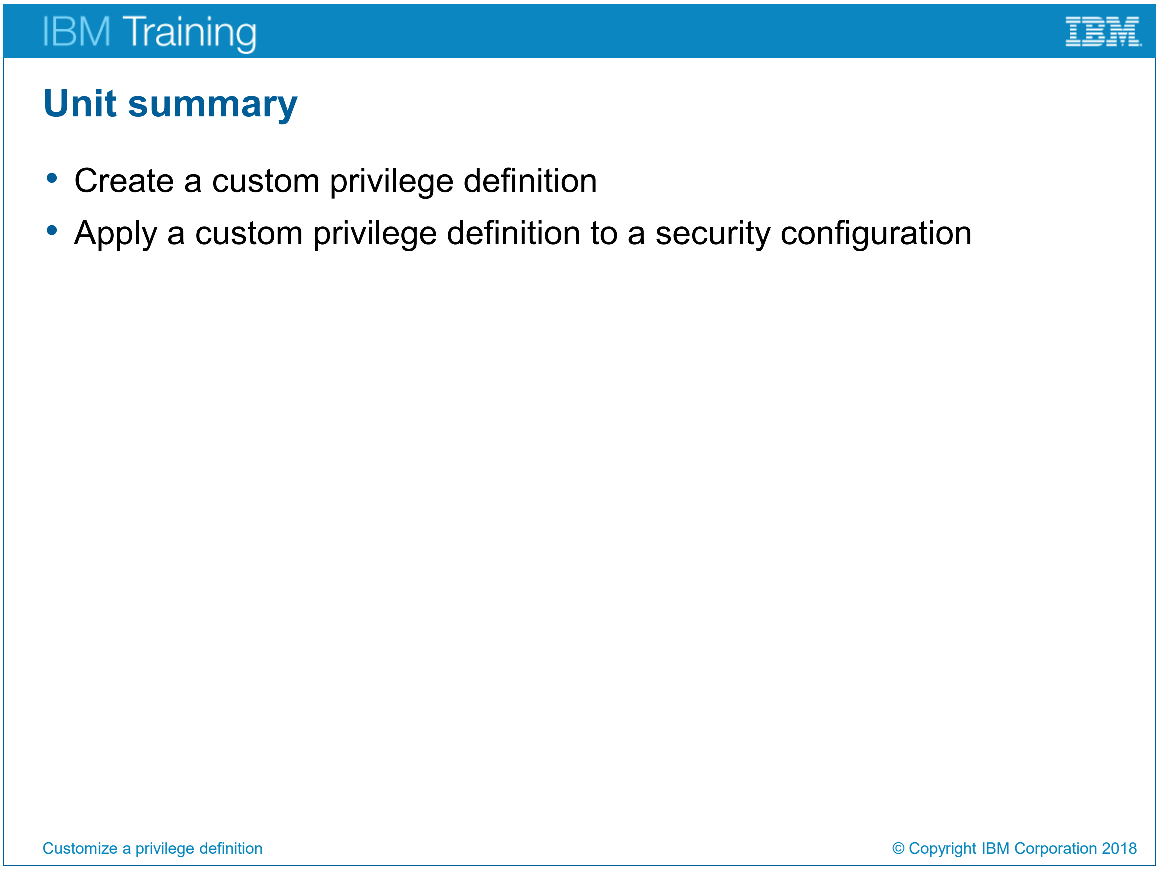
   

8. Click the **Tasks** tab, and verify that the **Add Task** button is inactive.

9. Click **Complete**, then log out of all applications and close all browsers.

Results:
You created a custom privilege definition by editing a security definition file, then applying that security definition to a solution. The resulting security definition included custom privileges that allowed insurance coordinators to complete tasks but did not allow them to add documents or comments or to start tasks.



IBM Training

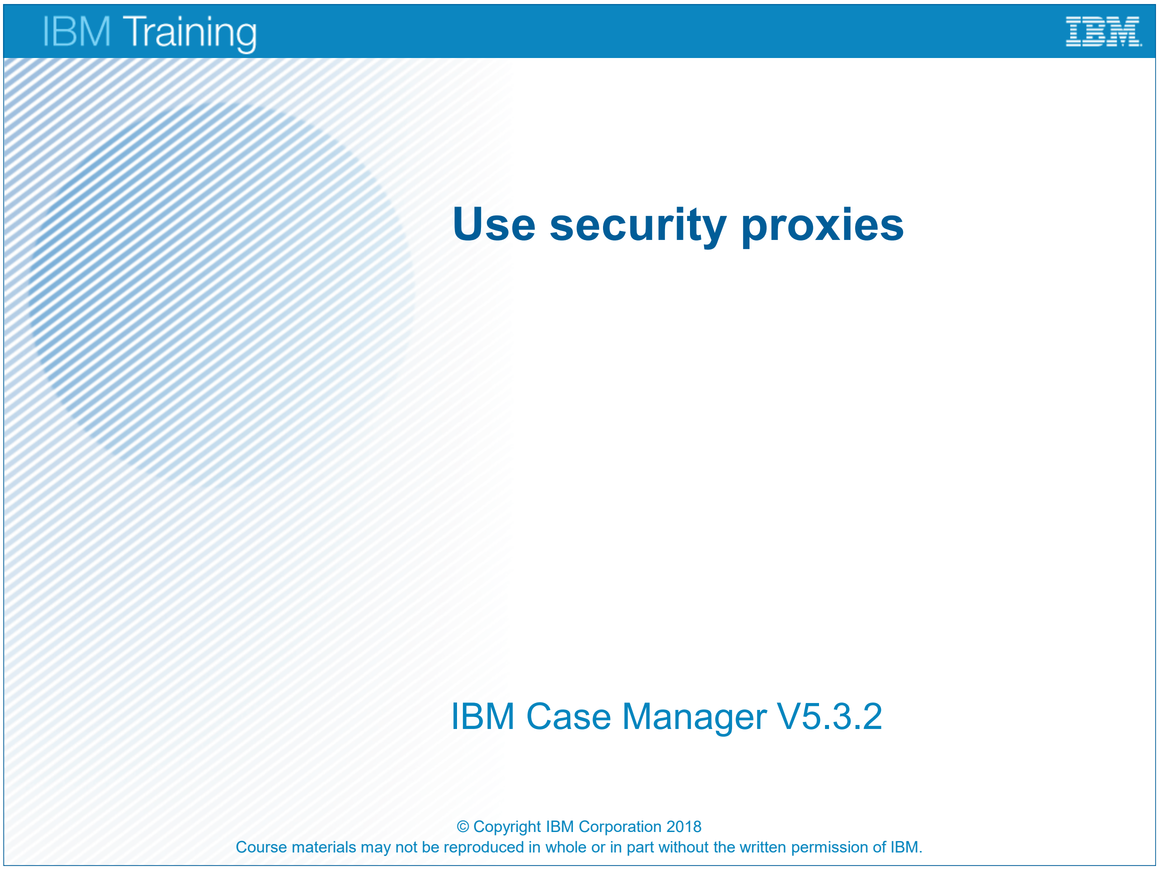
Unit summary

- Create a custom privilege definition
- Apply a custom privilege definition to a security configuration

Customize a privilege definition

Unit summary

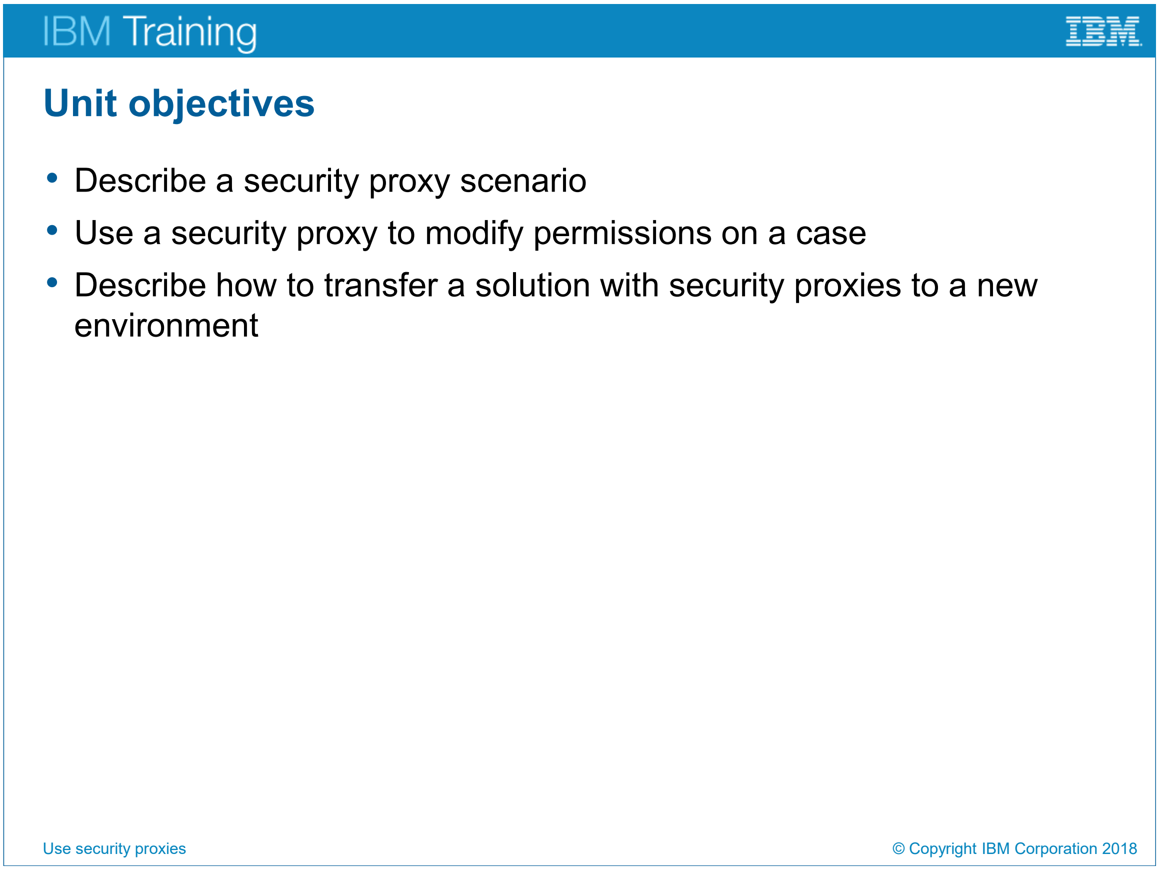
Unit 8 Use security proxies



IBM Training

Use security proxies

IBM Case Manager V5.3.2



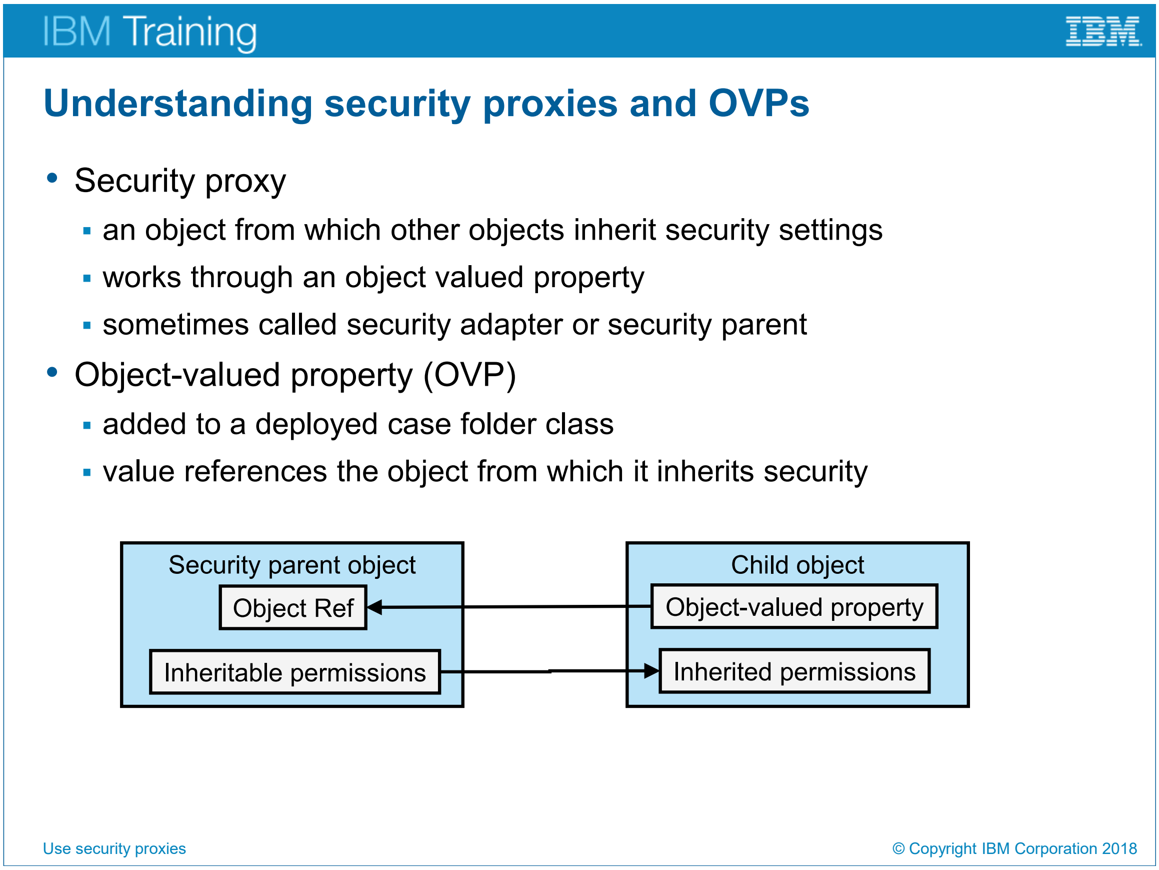
IBM Training

Unit objectives

- Describe a security proxy scenario
- Use a security proxy to modify permissions on a case
- Describe how to transfer a solution with security proxies to a new environment

Use security proxies

Unit objectives



IBM Training

Understanding security proxies and OVPs

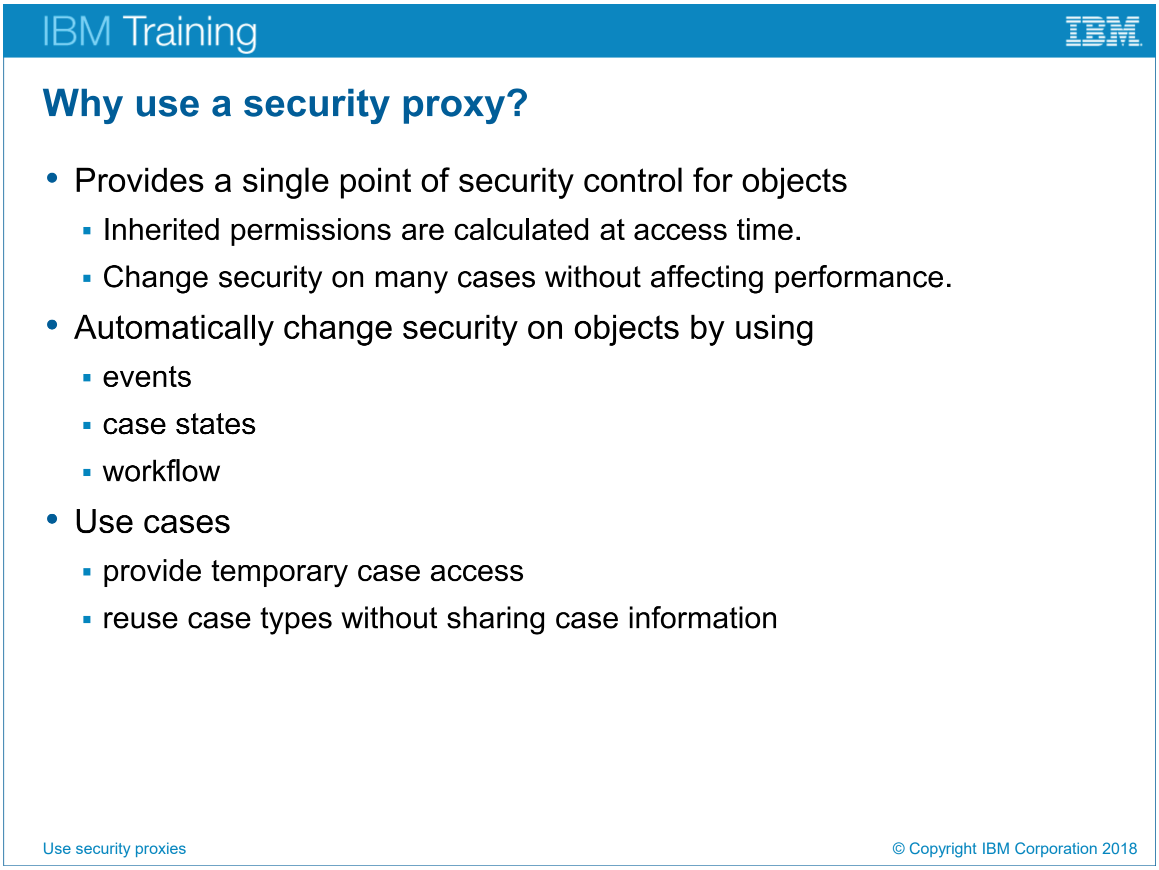
- Security proxy
  - an object from which other objects inherit security settings
  - works through an object valued property
  - sometimes called security adapter or security parent
- Object-valued property (OVP)
  - added to a deployed case folder class
  - value references the object from which it inherits security

Use security proxies

© Copyright IBM Corporation 2018

Understanding security proxies and OVPs

A security proxy is an object that other objects inherit security settings from. A security proxy works through an object valued property (OVP). The OVP is added to a deployed case folder class. The value of the OVP references the object from which it inherits its access control entry (ACE). Security proxies are sometimes called security adapters.



IBM Training

Why use a security proxy?

- Provides a single point of security control for objects
  - Inherited permissions are calculated at access time.
  - Change security on many cases without affecting performance.
- Automatically change security on objects by using
  - events
  - case states
  - workflow
- Use cases
  - provide temporary case access
  - reuse case types without sharing case information

Use security proxies

© Copyright IBM Corporation 2018

Why use a security proxy?

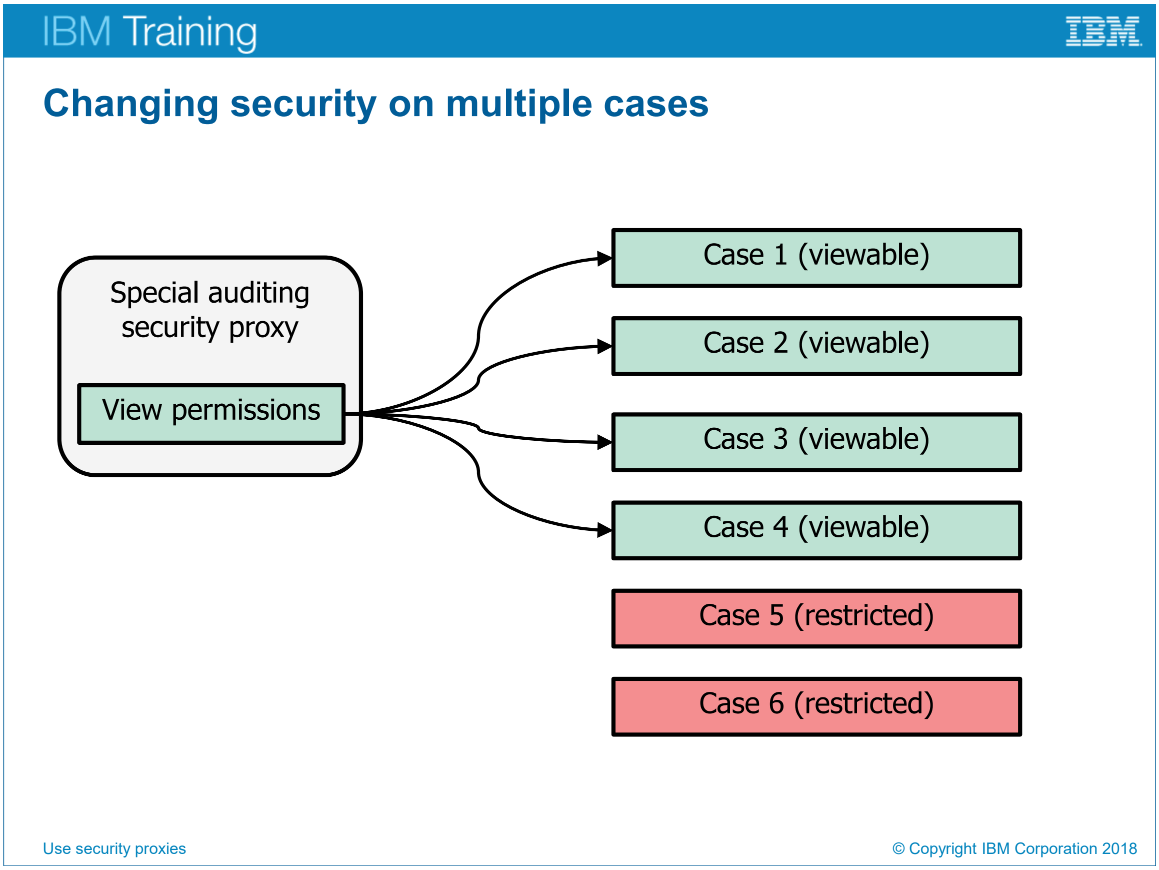
A security proxy provides a single point of control for objects. Security proxies use security inheritance to control access to other objects. Security proxies work through the security inheritance model. Access control entries (ACEs) are inherited from a parent object to child objects. Inherited security ACEs are evaluated when the object is accessed, so there is no extra processing when you change security settings.

Security proxies are useful for objects with changing security requirements. With security proxies, you can:

- Change inherited permissions on many cases without a processing cost.
- Use a security proxy to instantly add or remove authorization to many cases at the same time.
- Automate security changes by changing the value of the OVP to reference an object with different security settings.
- You can create security proxies for different scenarios and reuse them.

For example, you might want to allow an auditor temporary view access to a case. You can set the security proxy to give auditors permissions. When you set the security proxy object as the parent proxy for a case, the auditors can view the case. Later, you can change or delete the value of the OVP to remove the access. By using security proxies, you can change security on an individual case, or multiple cases.

In another example, you have a large company with many organizations. Each organization can use the same case type, but it is important to prevent organizations from seeing one another's cases. To accomplish this goal, you can create a security adapter hierarchy that matches your organizational structure. You can then use automation to assign security adapters to cases during run time.



IBM Training

Changing security on multiple cases

Special auditing security proxy

View permissions

Case 1 (viewable)

Case 2 (viewable)

Case 3 (viewable)

Case 4 (viewable)

Case 5 (restricted)

Case 6 (restricted)

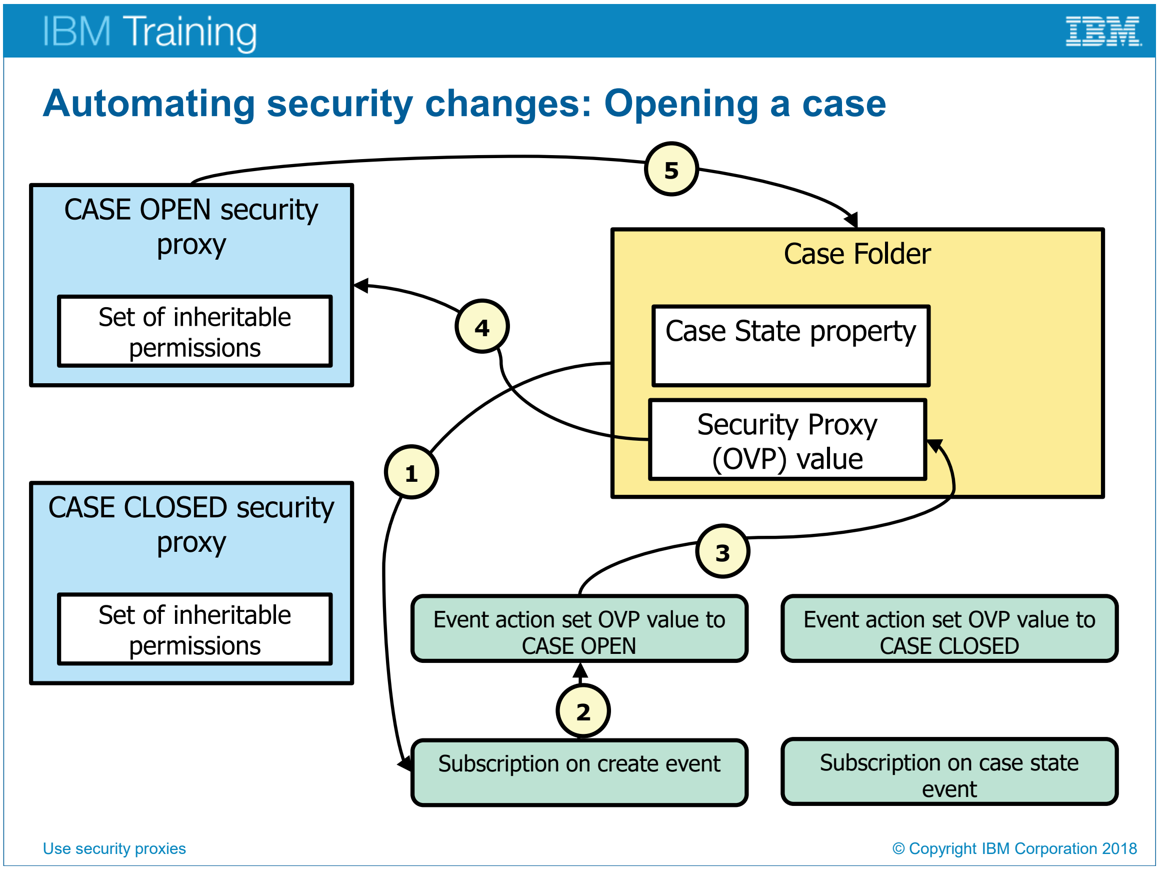
Use security proxies

© Copyright IBM Corporation 2018

Changing security on multiple cases

You can use a security proxy object to provide the same permissions to multiple cases. All of the cases with the reference to the security proxy can inherit permissions to allow extra access. The cases that do not include the reference do not have these permissions, so they have default permissions.

You can refine your security model by creating several security proxy objects with different sets of inheritable permissions. Each case can then include a reference to the proxy object with the desired set of permissions.



IBM Training

Automating security changes: Opening a case

CASE OPEN security proxy

Set of inheritable permissions

CASE CLOSED security proxy

Set of inheritable permissions

Case Folder

Case State property

Security Proxy (OVP) value

Event action set OVP value to CASE OPEN

Event action set OVP value to CASE CLOSED

Subscription on create event

Subscription on case state event

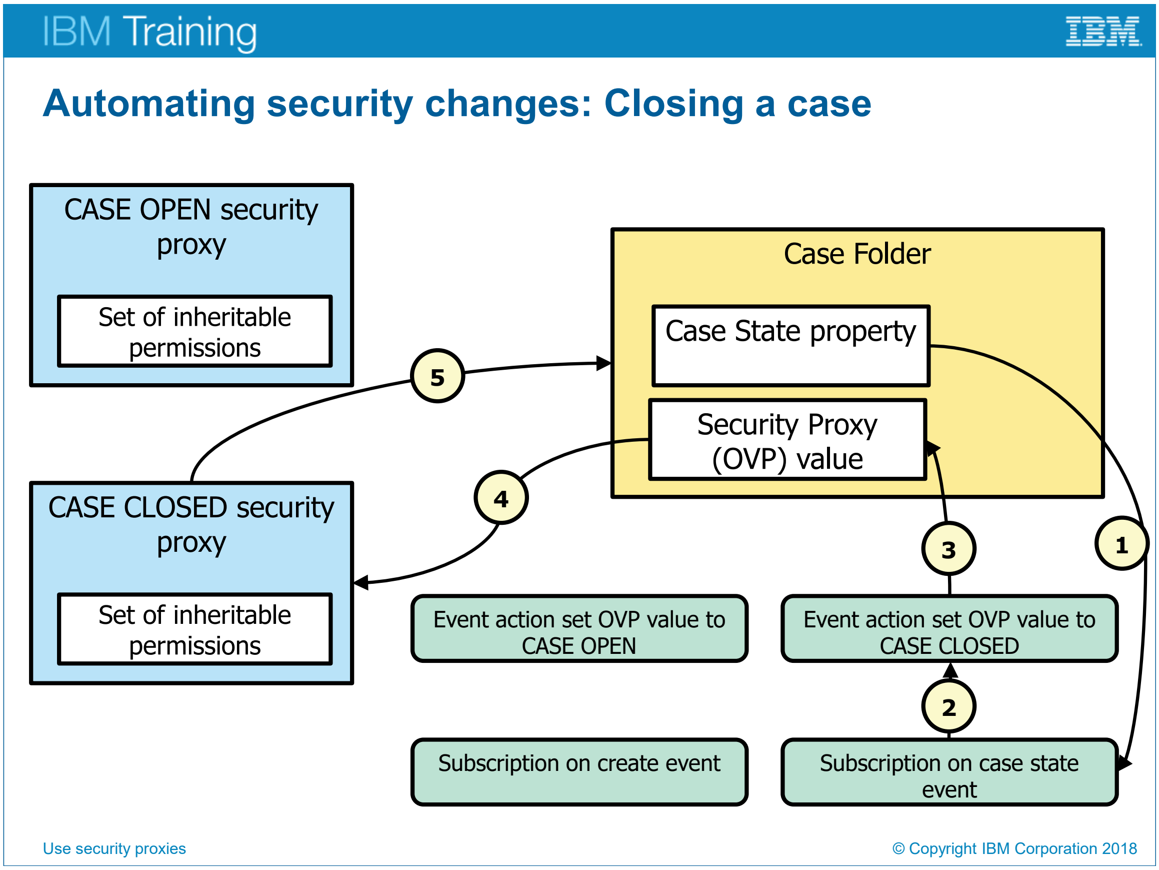
Use security proxies

Automating security changes: Opening a case

The diagram shows one way to automate security changes on a case by using a security proxy.

A solution architect wants a way to change the security of a case folder when a case is closed, so that after the case is closed, users would be unable to change case properties. The solution architect uses a combination of security proxies and event subscriptions to achieve this goal. The first part of the solution requires that the case folder obtain initial security settings when the case is opened. When the case is closed, the case switches to a different security proxy, thereby changing the inherited case folder security settings.

1. When the case is opened, IBM Case Manager creates a case folder. The creation event has a subscription associated with the case folder class.
2. The event subscription activates an event action.
3. The event action changes the value of the security proxy object-valued property (OVP) reference.
4. The new value of the object-valued property points to the CASE OPEN security proxy object.
5. The case folder inherits security settings from the CASE OPEN security proxy.



IBM Training

Automating security changes: Closing a case

CASE OPEN security proxy

Set of inheritable permissions

CASE CLOSED security proxy

Set of inheritable permissions

Case Folder

Case State property

Security Proxy (OVP) value

Event action set OVP value to CASE OPEN

Event action set OVP value to CASE CLOSED

Subscription on create event

Subscription on case state event

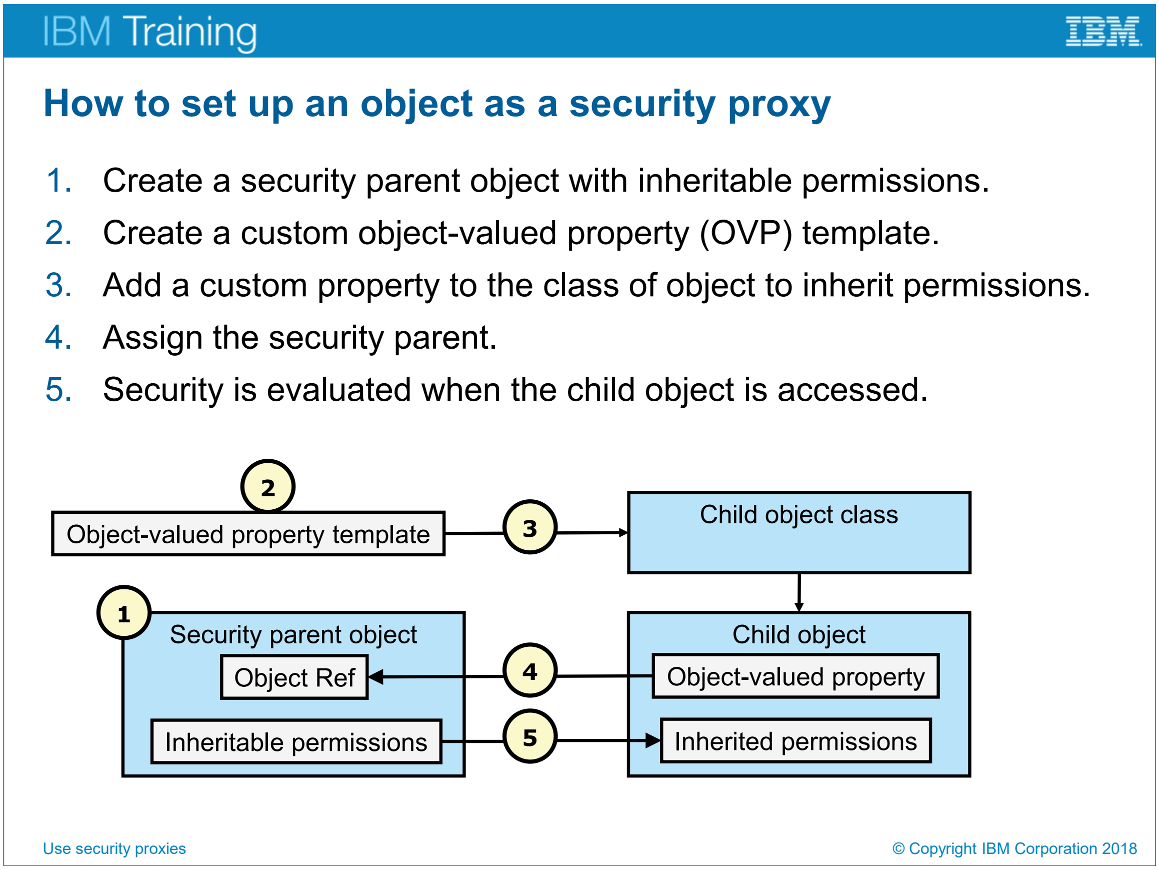
Use security proxies

Automating security changes: Closing a case

The diagram shows one way to automate security changes on a case by using a security proxy.

A solution architect wanted a way to have the security of a case folder change when a case is closed so that after the case is closed, users would be unable to change case properties. The solution architect used a combination of security proxies and event subscriptions to achieve this goal. The second part of the solution shows what happens when the case is closed. The case switches to a different security proxy, thereby changing the inherited case folder security settings.

1. When the case is closed, the change in the case state property triggers an event subscription.
2. The event subscription activates the event action.
3. The event action changes the value of the security proxy object-valued property (OVP) reference.
4. The new value of the object-valued property points to the CASE CLOSED security proxy object.
5. The case folder inherits security settings from the CASE CLOSED security proxy.



IBM Training

IBM

How to set up an object as a security proxy

1. Create a security parent object with inheritable permissions.
2. Create a custom object-valued property (OVP) template.
3. Add a custom property to the class of object to inherit permissions.
4. Assign the security parent.
5. Security is evaluated when the child object is accessed.

2

Object-valued property template

3

Child object class

1

Security parent object

Object Ref

Inheritable permissions

4

5

Child object

Object-valued property

Inherited permissions

Use security proxies

© Copyright IBM Corporation 2018

How to set up an object as a security proxy

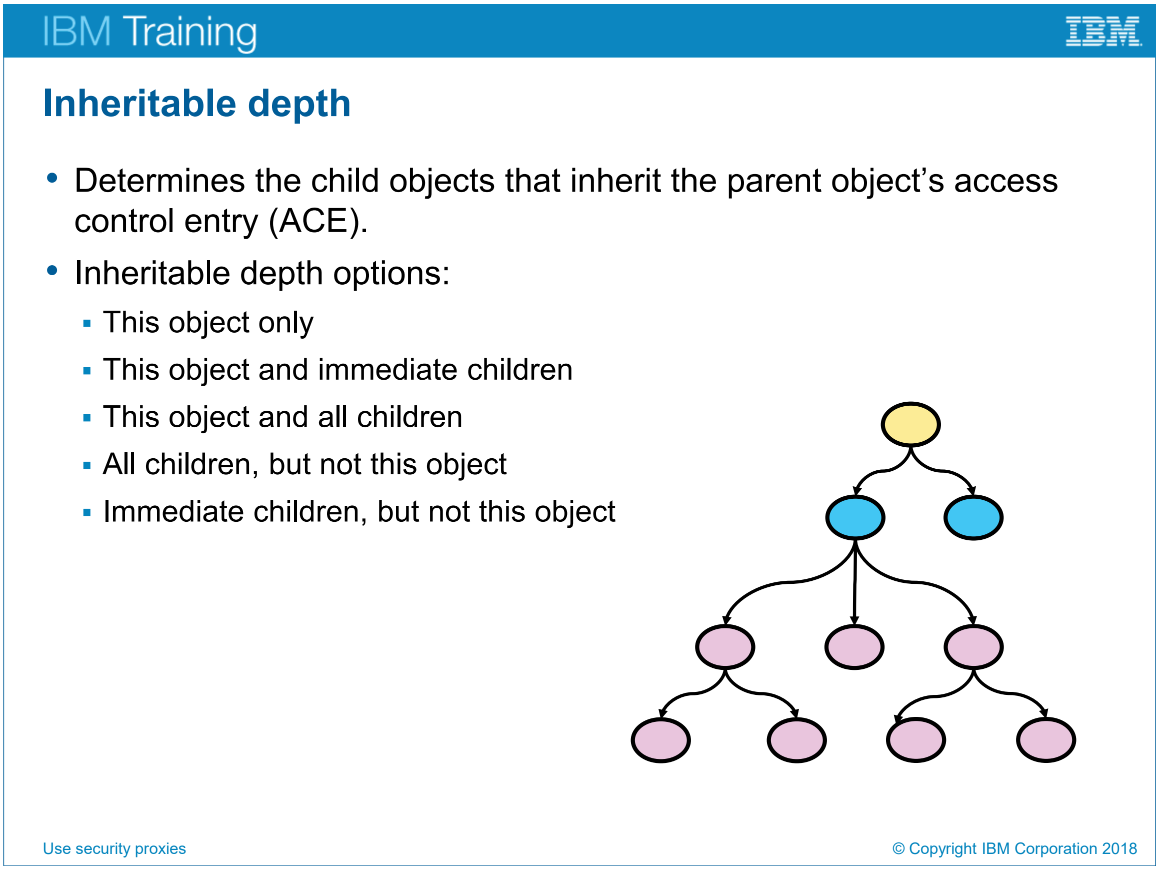
The graphic shows a high-level overview of the process for setting up an object as a security proxy. The Content Platform Engine provides a way to create objects to act as security proxies. This method is more complex than using folder inheritance, but it provides more flexibility. You can specify as many security parents as you need, and the security sources are not limited to folders. For some business applications, the freedom to use other objects besides folders might allow for a more natural and simpler solution. This method can also be combined with folder inheritance so that the final security on an object includes the inherited security from all sources.

The object valued property must be single-valued. The security proxy type is inherited.

To use a security proxy, create a custom property on the child class of the object-valued property type. The object-valued property has a required class. For required class, select the exact class of the parent object.

If the security proxy object is changed, the inherited security is updated to the new security settings.

If the security parent object is deleted, the inherited security is removed from the object.



IBM Training

Inheritable depth

- Determines the child objects that inherit the parent object’s access control entry (ACE).
- Inheritable depth options:
  - This object only
  - This object and immediate children
  - This object and all children
  - All children, but not this object
  - Immediate children, but not this object

Use security proxies

© Copyright IBM Corporation 2018

Inheritable depth

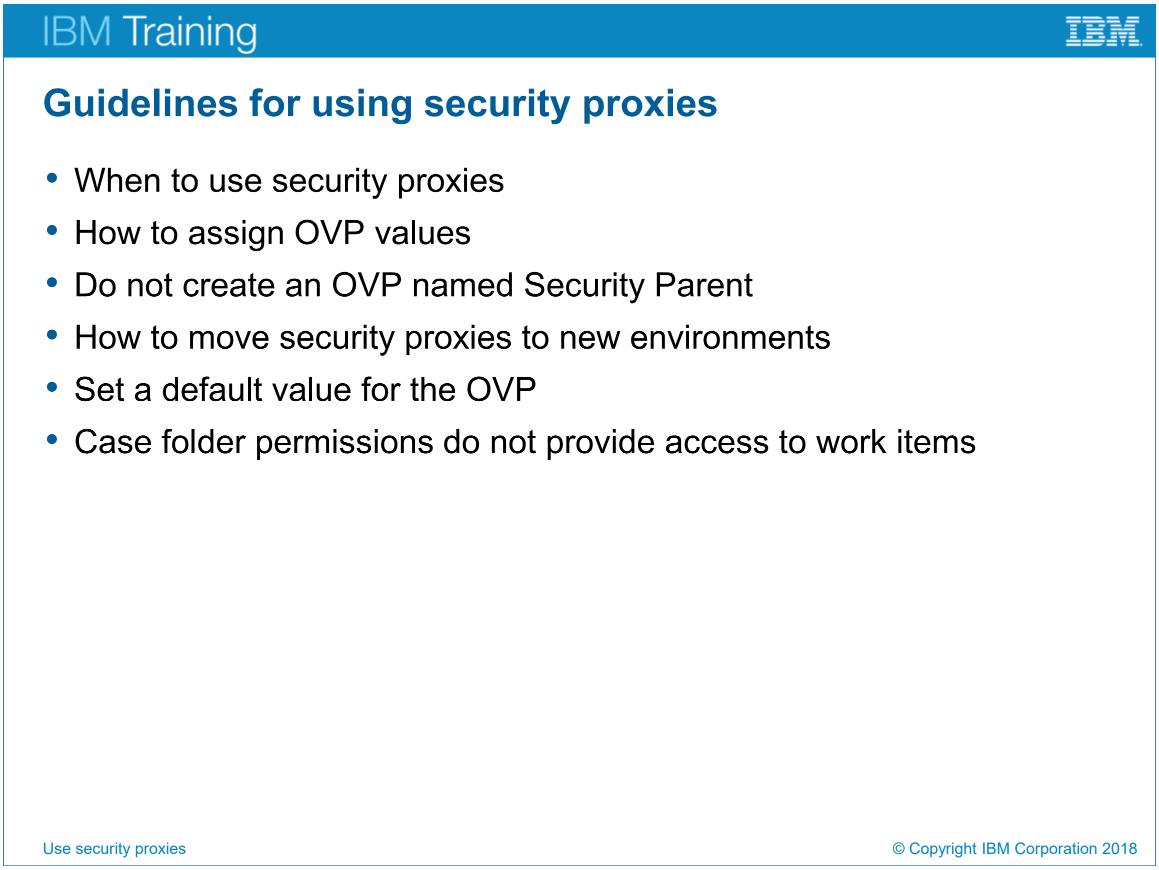
When you set security to be inherited, you must consider the inheritable depth. Inheritable depth determines the child objects that inherit the parent object’s access control entry (ACE).

You can set the inheritable depth on a security proxy so that security settings apply to child objects in the following ways:

- This object only: This ACE is not inherited even if the child is configured for inheritance.
- This object and immediate children: This ACE applies to the object and is inherited by the child objects, but not by the child object's children. The child ACE has an inheritable depth of This object only.
- This object and all children: This ACE applies to the object and is inherited by every generation of the parent object's child objects.
- All children, but not this object: This ACE is inherited by every generation of the parent object's child objects, but does not affect the parent object itself.
- Immediate children, but not this object: This ACE is inherited only by the parent object's immediate children, but not by further generations, and does not affect the parent object itself.

Use the *All children, but not this object* option to inherit permissions from objects that do not contain those permissions themselves. For example, custom objects do not have content, but modify content permissions are available for inheritance.

You can also use this setting to prevent users who have full control over child objects from altering a security proxy.



IBM Training

Guidelines for using security proxies

- When to use security proxies
- How to assign OVP values
- Do not create an OVP named Security Parent
- How to move security proxies to new environments
- Set a default value for the OVP
- Case folder permissions do not provide access to work items

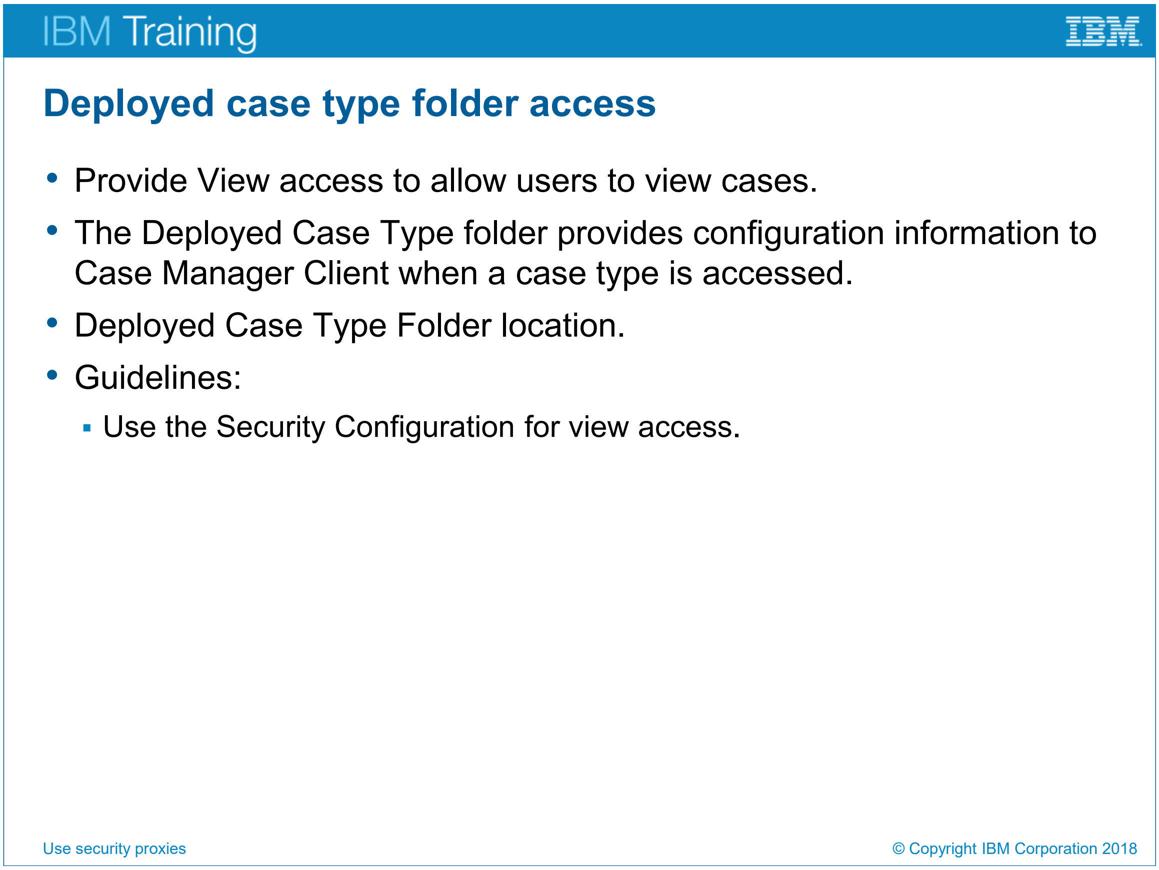
Use security proxies

© Copyright IBM Corporation 2018

Guidelines for using security proxies

Consider the following guidelines for using security proxies:

- Use security proxies when you need to be able to dynamically control access to cases.
- Use automation to assign security proxies when the case is created.
- Do not create an OVP named Security Parent because it is a reserved property name.
- Security proxies and OVPs exist only in the target object store, so they are not part of the Solution Definition File (SDF). You must move them by using FileNet Deployment Manager.
- Set a default value for the OVP if you want to provide dynamic control for all instances of a case type.
- Remember that the case folder object does not provide access to work items. To provide access to work items, you must configure security on the workflow system.



IBM Training

Deployed case type folder access

- Provide View access to allow users to view cases.
- The Deployed Case Type folder provides configuration information to Case Manager Client when a case type is accessed.
- Deployed Case Type Folder location.
- Guidelines:
  - Use the Security Configuration for view access.

Use security proxies

© Copyright IBM Corporation 2018

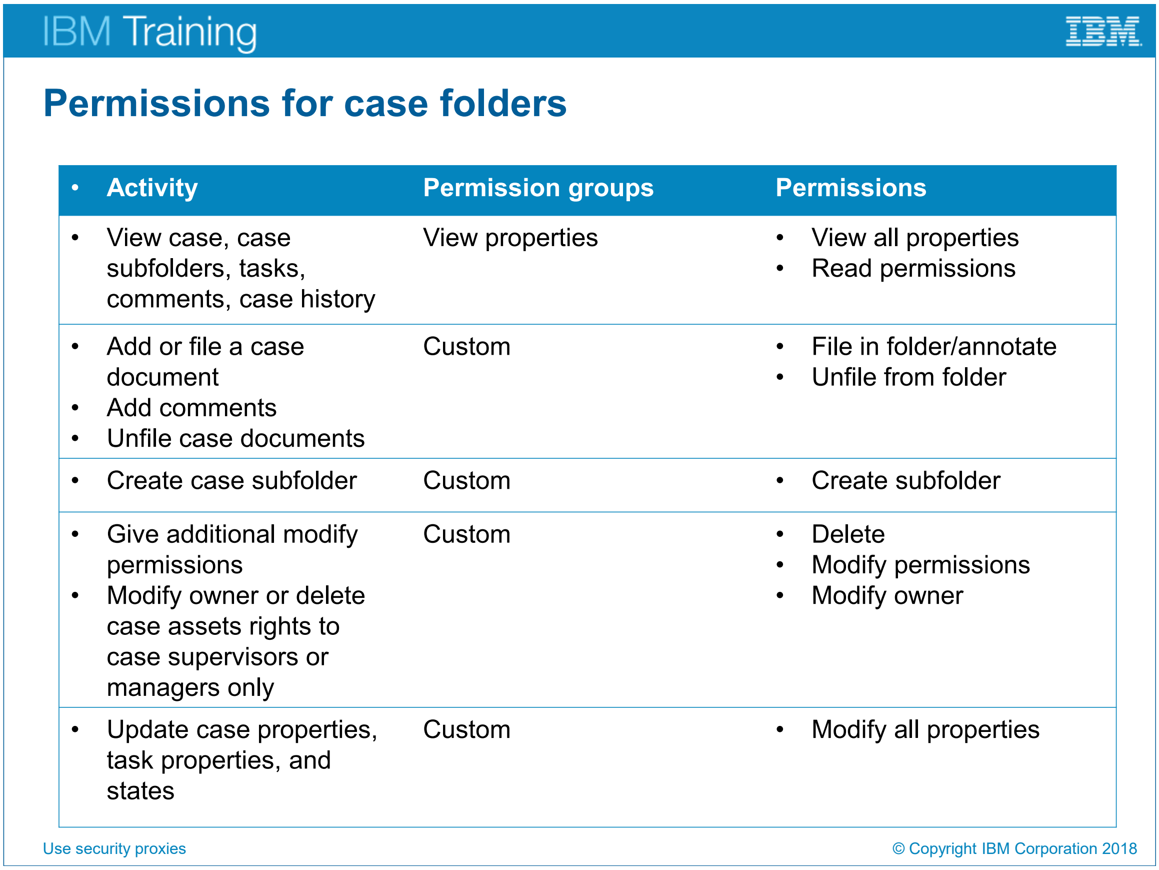
Deployed case type folder access

Use Administration Console for Content Platform Engine to find the Deployed Case Type folder:

> *Target Object Store* > Browse > Root Folder > IBM Case Manager > Solution Deployments > *Solution Name* > Case Types > Case Type Folder
>
> – Where Solution Name is the name of your solution.

Use these guidelines when you use security proxies:

- If possible, use the Security Configuration to give all users who might open a case at least View access. This setting automatically provides View access to the Deployed Case Type folder. If you do not provide View access to the Deployed Case Type folder, then users cannot access the case.
- If you want to control View access to a case with a security proxy, you must grant View permissions directly on the Deployed Case Type folder. Grant access to the object store master group on the Deployed Case Type folder. For inheritable depth, use the *This Object Only* setting so that View permissions are not inherited down to the individual cases.



IBM Training

Permissions for case folders

• Activity	Permission groups	Permissions
• View case, case subfolders, tasks, comments, case history	View properties	• View all properties • Read permissions
• Add or file a case document • Add comments • Unfile case documents	Custom	• File in folder/annotate • Unfile from folder
• Create case subfolder	Custom	• Create subfolder
• Give additional modify permissions • Modify owner or delete case assets rights to case supervisors or managers only	Custom	• Delete • Modify permissions • Modify owner
• Update case properties, task properties, and states	Custom	• Modify all properties

Use security proxies

Permissions for case folders

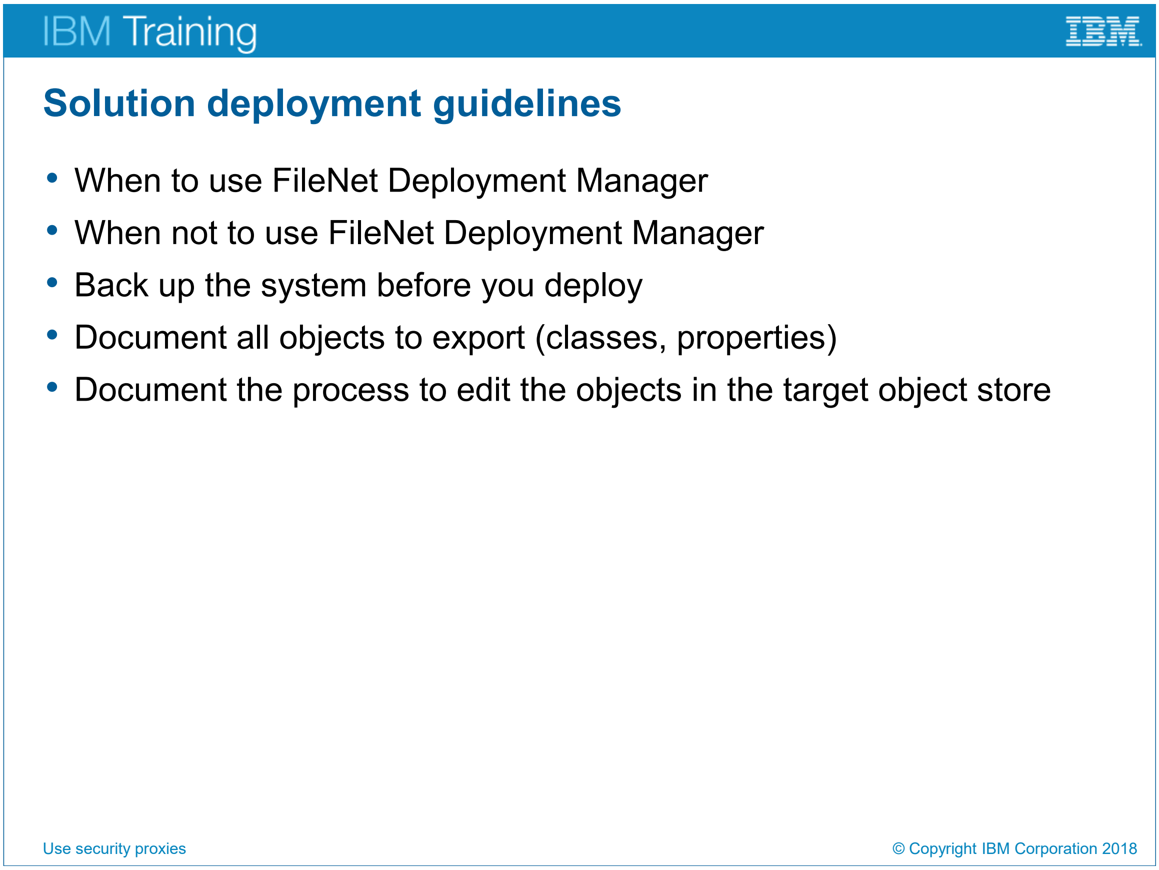
The table shows the permissions that are needed to perform case activities. Set the permissions on the security proxy correctly in order to achieve the expected results on the case type folder.

By default, the deployed case type folder instance has no security set. The table shows the permissions that are needed to perform case activities.

Security proxies affect the security of the deployed case type folder. You must set the permissions on the security proxy correctly to achieve the expected results on the case type folder.

For example, if you want to allow a group View Only permissions for cases, then you specify the following permissions: View all properties and Read permissions. Because you are setting the permissions on a security proxy, ensure that the inheritable depth is set to All children, but not this object.

Permission groups are groups of permissions that are often used together. You can select one of these permission groups to quickly set permissions. However, if the permission group does not have the exact permissions that you want, you can add or remove individual permissions. If you change the individual permissions after selecting a permission group, the permission group field displays Custom.



IBM Training

Solution deployment guidelines

- When to use FileNet Deployment Manager
- When not to use FileNet Deployment Manager
- Back up the system before you deploy
- Document all objects to export (classes, properties)
- Document the process to edit the objects in the target object store

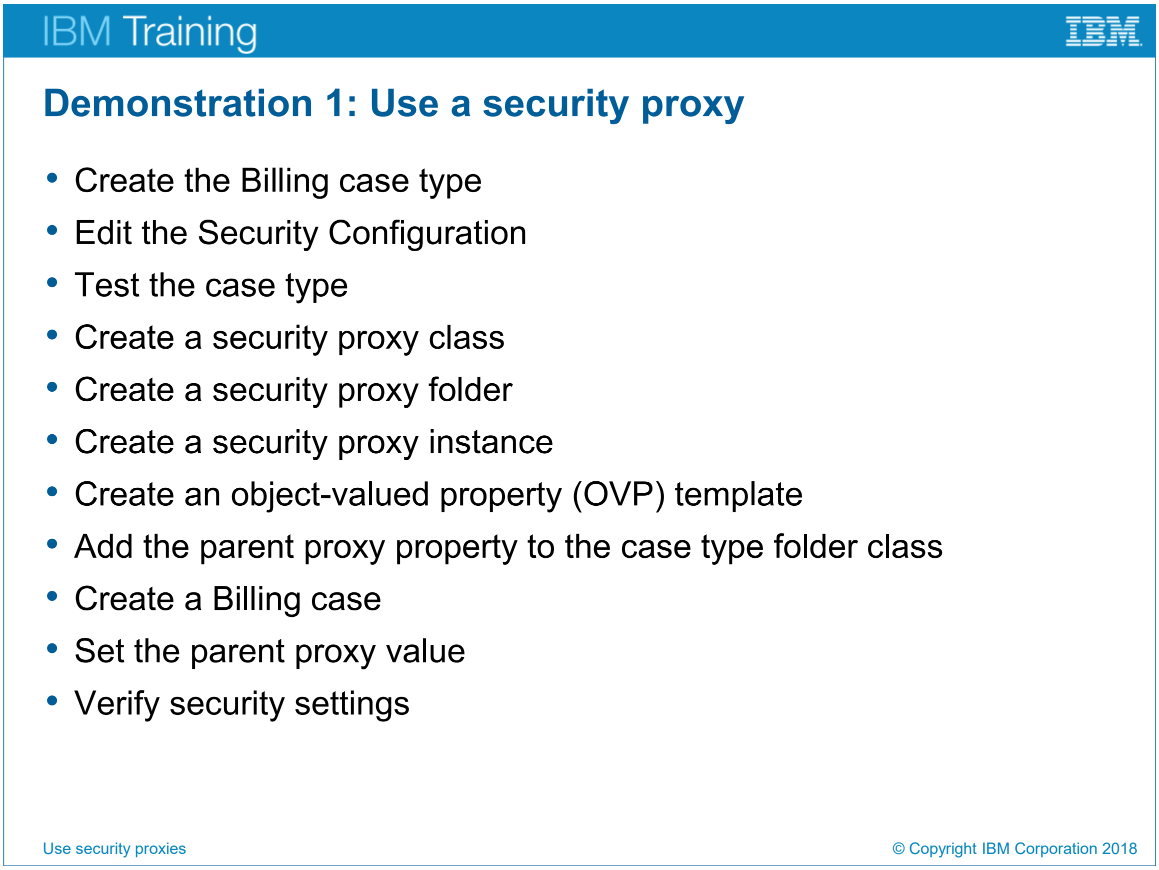
Use security proxies

© Copyright IBM Corporation 2018

Solution deployment guidelines

Use these guidelines to migrate a solution with security proxies:

- Security proxy objects, security proxy classes, object-valued properties are FileNet P8 assets. Use FileNet Deployment Manager (FDM) to transfer them when you migrate and deploy your solution in a new environent.
- Do not migrate altered Case Manager objects with FDM. If you customize a Case Manager artifact, such as a case folder class, do not attempt to move it with FDM.
  - If you altered solution objects in the Development environment, you must re-alter them in the non-development environment.
  - Carefully document the process so that it can be repeated.
- Import the solution objects with Case Manager administration client.
- Import FileNet P8 assets (security proxy objects, OVPs) by using FDM.



IBM Training

Demonstration 1: Use a security proxy

- Create the Billing case type
- Edit the Security Configuration
- Test the case type
- Create a security proxy class
- Create a security proxy folder
- Create a security proxy instance
- Create an object-valued property (OVP) template
- Add the parent proxy property to the case type folder class
- Create a Billing case
- Set the parent proxy value
- Verify security settings

Use security proxies

© Copyright IBM Corporation 2018

Demonstration 1: Use a security proxy

Demonstration 1: Use a security proxy

Purpose:
You are designing a Billing case type. Billing cases sometimes allow members of the Accounting group to access cases. You can provide access to cases by adding a security proxy to the case folder. Accountants can then access case information until you remove their access.

Case Manager Builder: **http://vclassbase:9081/CaseBuilder**

Case Admin client URL: **http://vclassbase:9081/navigator/?desktop=icmadmin**

ACCE URL: **http://vclassbase:9080/acce/**

Target object store: **DEV_Target_2**

Solution builder account: **Paula/FileNet1**.

Administrator account: **p8admin/FileNet1**

Task 1. Create the Billing case type.

The Billing case type serves as a placeholder for testing security. You are also going to add a role for Accountants to test the security scenario.

1. Log on to **Case Manager Builder** as **Paula/FileNet1**.
2. Edit the **Medical Visit** solution.
3. Create a role named **Auditor,** using the option: **Do not show common or role personal in-baskets**.
4. Create the **Billing** case type and **Bill Insurance** task by using the following information.

Page	**Property**	**Data**
Case type	Case type name	Billing
Properties	Name	Client Name
Views	Include in Case Summary	Client Name
Tasks	Task name	Bill Insurance

Task 2. Edit the Bill Insurance task.

1. Open the **Bill Insurance** task in **Step Editor**.
2. Add a **Role Lane** for **Insurance Coordinator**.

3. Add a step named **Bill Insurance** to the **Insurance Coordinator** role lane, and add the **Client Name** property to the step.
4. Connect the **Launch** step to **the Bill Insurance Step**.
5. **Save** and close the task.
6. **Validate** the case type.
7. **Save and Close**.
8. **Redeploy** the solution and wait for the operation to complete.
9. Log out of **Case Manager Builder**.

Task 3. Edit the security configuration.

The Security Configuration does not currently include security for the new case type. You are going to edit the Security Configuration to allow Insurance Coordinators to create and manage Billing cases.

1. Log in to **Case Manager administration client** as **p8admin/FileNet1**.
2. Open the **DEV_design** object store and then select **Solutions**.
3. In the main pane, click **Medical Visit** solution, then click **Actions** > **Manage** > **Security Configuration**.
4. Select **Edit a security configuration**, and then select **MEDSEC**, and then click **Next** twice to get to the **Modify permissions for roles** page.
5. Click **Add**, select the **Billing** case type, then click **Add**, then scroll down and expand the **Billing** case type.
6. For **Insurance Coordinator** in the **Billing** case type, select the **Create Case** and **Manage Case** permissions.
7. Click **Next** until you get to **Associate users and groups with roles**.
8. Scroll down and select the **Auditor** role, and then click **Add**.

   You might need to use the scroll bars to show the Add button.
9. Add the **Accounting** group to the role, and then click **Next**.

   Remember to select Groups when you search.
10. On the **Apply the security configuration** page, select **Apply the security configuration**, then click **Apply**.
11. Wait for a Success message, and then click **Close**, then log out of **Case Manager administration client**.

Task 4. Test the case type.

Verify that you can add a Billing case.

1. Log on to **Case Manager Client** as **Addington/FileNet1**.
2. Click **Add Case** > **Billing**.
3. Type the client name, `Bill`, and then click **Add**.

4. Open the **Work** tab to verify that the step is in your in-basket.
5. Open and complete the step.
6. Log out of **Case Manager Client**.

Task 5. Configure a security proxy class.

You are going to use a custom object to be a security proxy for your cases. You must create this class before you can create individual security parents.

1. In **Firefox**, click the **ACCE** link on the home page to log on to **Administration Console for Content Platform Engine** as **p8admin/FileNet1**.
2. Open the **DEV_Target_2** object store.
3. Navigate to and select **Data Design** > **Classes** > **Custom Object**.
4. Click **Actions** > **New Class**.
5. On the **Name and Describe the Class** page, type **`Security Proxy`**, then click **Next**.
6. On the **Summary** page: click **Finish**, then click **Close**.

Task 6. Create a security proxy folder.

In this procedure, you create a folder to contain security proxy objects. Keep your security proxies in one location so that you can easily find and administer them. You are logged in to **Administration Console for Content Platform Engine**.

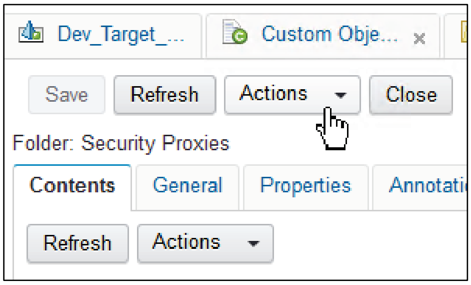
1. In the **DEV_Target_2** object store, navigate to **Browse** > **Root Folder**.
2. Click **Actions** > **New Folder**.
3. Name the folder: **`Security Proxies`**.
4. Complete the wizard with default settings.
5. Open the folder.

Task 7. Create a security proxy object.

In this task, you create an instance of the security proxy class. You must set the security to be inherited and configure View permissions. You are in the Security Proxies folder that you created in the previous procedure.

1. Click **Actions** > **New Custom Object**.

   Make sure that you click the top **Actions** button.



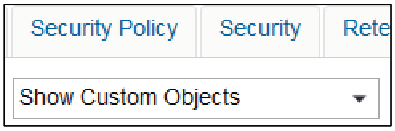
Folder: Security Proxies

2. On the **Define a Custom Object** page, enter the following information then click **Next**:
   - **Containment Name**: **Auditing Security Object**.
   - **Class**: **Security Proxy**.
3. Complete the wizard by clicking **Next** several times, then click **Finish**. Click **Close**.

Task 8. Edit the security proxy object permissions.

After you create the object, you can modify the inheritable permissions. By default, the folder shows only documents, so you must first choose to show custom objects.

1. In the toolbar, select **Show Custom Objects** from the menu.



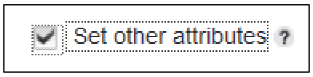
2. Click the **Auditing Security Proxy**.
3. Open the **Security** tab.
4. Click **Add User/Group Permission**.
5. Search for group: **Accounting**.
6. Add the **Accounting** group to the **Selected Users and Groups** list.
7. Scroll down to select the following settings:
   - **Apply to: All children but not this object.**
   - **Permission group: View properties <Default>**
8. Click **OK**, then save your changes.

Task 9. Create an object-valued property template.

In this task you create an object valued property. This property can be configured to reference the security proxy object. It is critical that you select the Set Other Attributes check box, so that you can set the Security Proxy Type value. You are logged on to *Administrative Console for Content Platform Engine*.

1. Navigate to **DEV_Target_2** > **Data Design** > **Property Templates**.
2. Click **New**.
3. In the **Display name** field, type `Parent Proxy`, then click **Next**.
4. In the **Data type** menu, select **Object**, then click **Next**.

5. On the **Single or Multi-Value** page, select **Set other attributes**, then click **Next**.



☑ Set other attributes

6. On the **Additional Property Template Attributes** page, configure the following settings, then click **Next**:
   - **Settability: Read-Write**
   - **Security Proxy Type: Inherited**
7. On the **Access Rights** page, click **Next**.
8. On the **Summary** page, click **Finish**.
9. Click **Close**.

Task 10. Add the OVP to the case type folder class.

In this task you add the object-valued property (Parent Proxy) to the Billing case type folder class. When someone creates a Billing case, the case folder has this property that references the security proxy. You are logged on to Administration Console for Content Platform Engine.

1. Open **DEV_Target_2** > **Data Design** > **Classes** > **Folder** > **Base Case** > **Case Folder** > **Billing**.
2. Open the **Property Definitions** tab.
3. Click **Add**, scroll down and select **Parent Proxy**, then click **OK**.
4. Click the **Parent Proxy Property Definition** to set property definition attributes.
5. Open the **More** tab.
6. In the **Required class** field, select **Security Proxy**. Be careful with your selection and ensure you choose the correct value from the list.
7. Click **Save**, then click **Close**.
8. Log out of **Administration Console for Content Platform Engine**.

Task 11. Create a Billing case and inspect security.

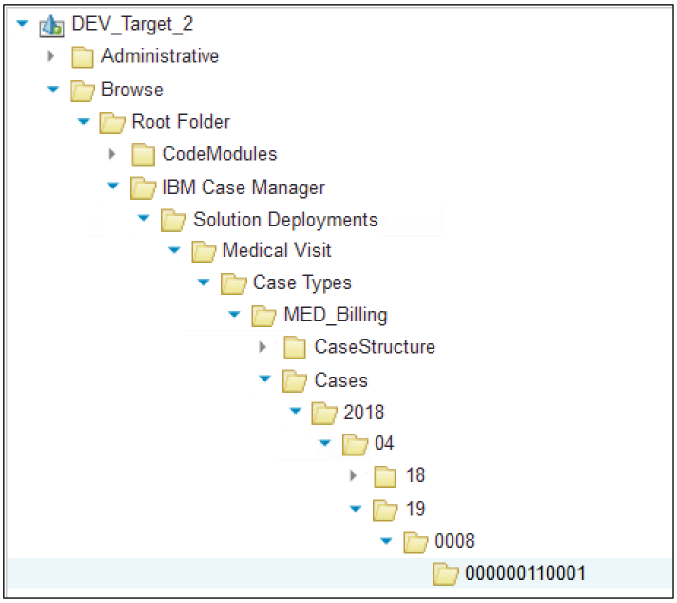
In this task, you create a Billing case instance to test security.

1. Log on to **Case Manager Client** as **Addington/FileNet1**.
2. Add a **Billing** case.
3. Client name: `Roxy`.
4. Leave the **Parent Proxy** value blank and then click **Add**.
5. Log out of **Case Manager Client**.
6. Log in to **Administration Console for Content Platform Engine** as **p8admin/FileNet1**.

7. Navigate to **DEV_Target_2 > Browse > Root Folder > IBM Case Manager > Solution Deployments > Medical Visit > Case Types > MED_Billing > Cases >** ***year*** **>** ***month*** **>** ***day*** **> random number >** ***case number***.

   Note: There may be multiple random number folders. Open each folder and check the case numbers. Select the latest case number folder, the one with the highest number.

   The results appear as follows:

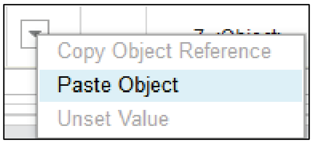


8. Open the **Security** tab.
9. Confirm that the **Accounting** group is not in the access control list.

Task 12. Set the parent proxy value.

You are going to set the value of the Parent Proxy property of the case type. After the value is set, the security of the case changes to reflect settings that are inherited from the security proxy. You are still logged in to *Administration Console for Content Platform Engine*.

1. Navigate to **DEV_Target_2** > **Browse** > **Root Folder** > **Security Proxies**.
2. Select **Show Custom Objects** to view custom objects in this folder.
3. Open **Auditing Security Object**.
4. Click **Actions** > **Copy Object Reference**.
5. Navigate back to the **Billing** case folder that you created in Task 11.
6. Open the **Properties** tab, and then scroll down to the **Parent Proxy** property.
7. Click the arrow and then select **Paste Object**, then click **Save**.

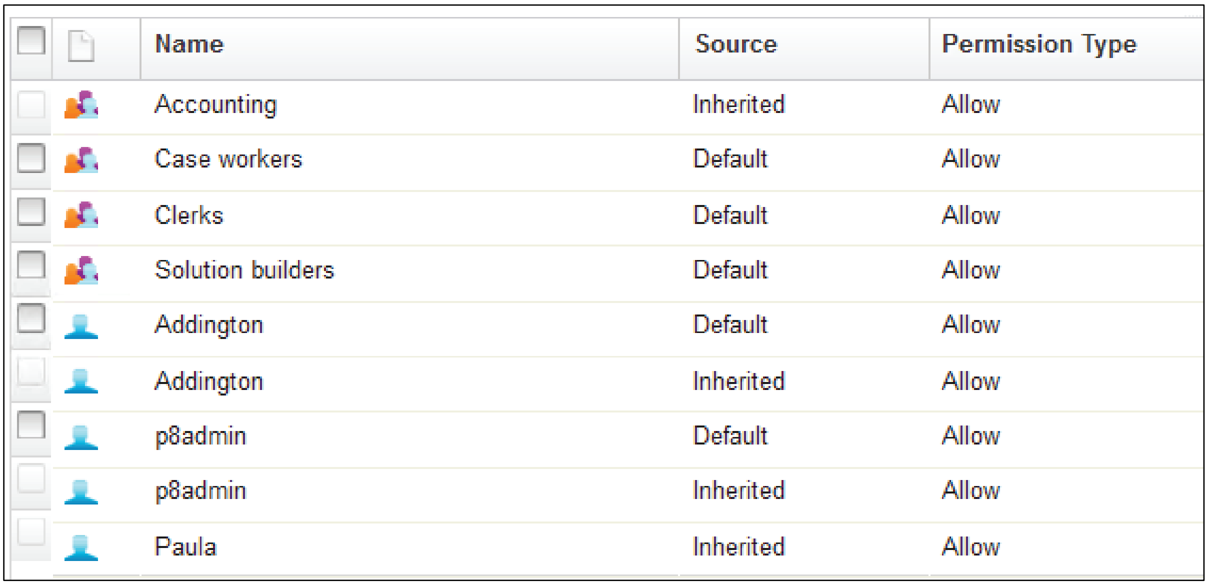


Task 13. Verify the security change.

You have changed the security on a single case folder by using a proxy object. To see the changes, you are going to view the security of the folder.

1. Click **Refresh** to refresh the case folder.
2. Open the **Security** tab.
3. Confirm that the **Accounting** group is in the access control list as an Inherited permission.

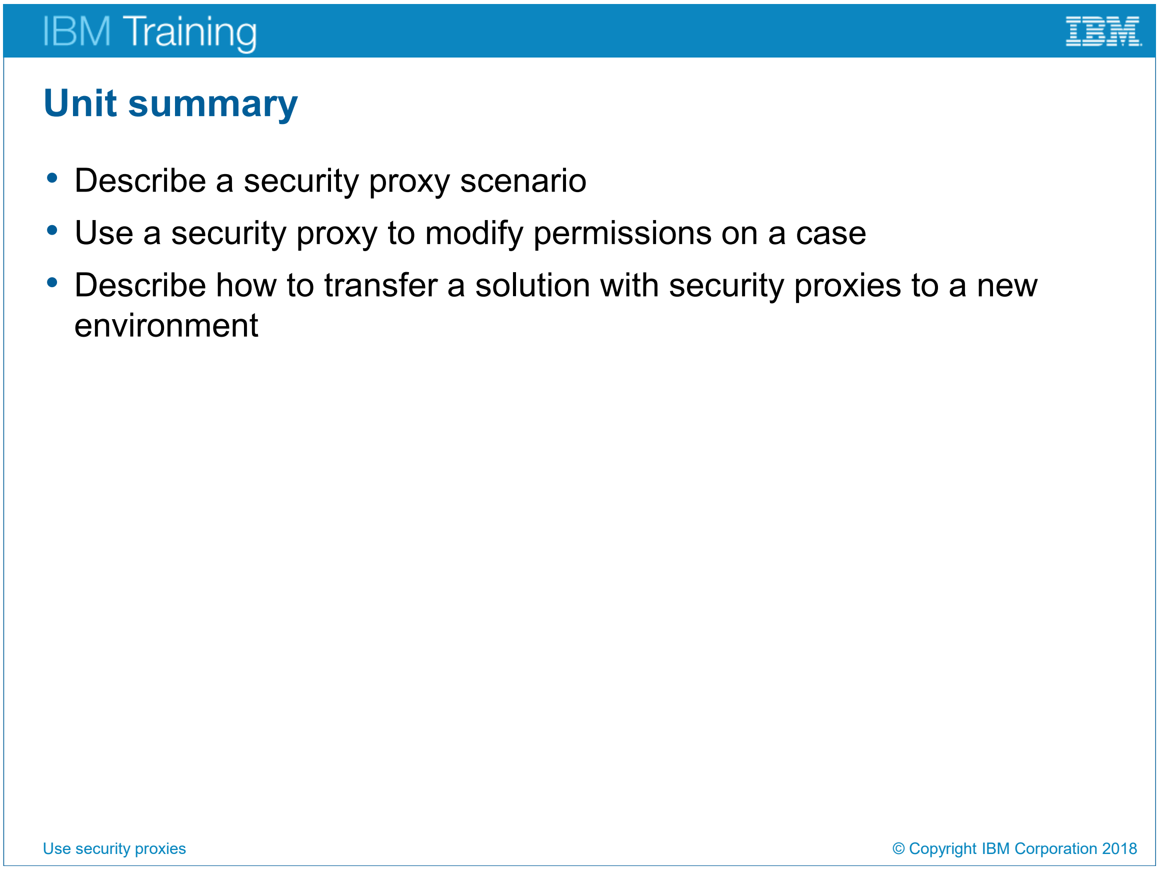
The results appear as follows:



□		Name	Source	Permission Type
□		Accounting	Inherited	Allow
□		Case workers	Default	Allow
□		Clerks	Default	Allow
□		Solution builders	Default	Allow
□		Addington	Default	Allow
□		Addington	Inherited	Allow
□		p8admin	Default	Allow
□		p8admin	Inherited	Allow
□		Paula	Inherited	Allow

4. Log out of all applications and close the browser.

Results:
You created a security proxy and an object-valued property. You used the security proxy to change the security on a case folder.



IBM Training

Unit summary

- Describe a security proxy scenario
- Use a security proxy to modify permissions on a case
- Describe how to transfer a solution with security proxies to a new environment

Use security proxies

© Copyright IBM Corporation 2018

Unit summary

IBM Training

Apply your knowledge

Use security proxies

Apply your knowledge

Apply your knowledge

In this lesson, you learned about applying security proxies to case folders and about exporting solutions that contain security proxies. Complete this quiz to confirm that you understand the concepts.

For each question, choose the best answer.

Questions

1. What can you use a security proxy to provide?

   a. Direct permissions

   b. Inherited permissions

   c. Security configurations

   d. Access control lists

2. You want to use a security proxy to affect the security of a single case. Which object does the security proxy affect?

   a. Object-valued property

   b. Case folder class

   c. Security configuration

   d. Case folder

3. What connects the secured object to the security proxy?

   a. Object-valued property

   b. Security definition

   c. Security configuration

   d. Hyperlink

4. You are exporting a solution that has security proxies to a new environment. Which objects do you use Case Manager Administration Client to export? Choose more than one.

   a. Security configuration

   b. Security proxies

   c. Solution definition

   d. Object-valued properties

5. How do you export and import altered solution objects, such as case-type folders, to a new environment?

   a. Use Case Manager administration client

   b. Use FileNet Deployment Manager

   c. FileNet Enterprise Manager

   d. You do not

Answers

1. What can you use a security proxy to provide?

   b. Inherited permissions – correct answer

2. You want to use a security proxy to affect the security of a single case. Which object does the security proxy affect?

   d. Case folder – correct answer

3. What connects the secured object to the security proxy?

   a. Object-valued property – correct answer

4. You are exporting a solution that has security proxies to a new environment. Which objects do you use Case Manager Administration Client to export? Choose more than one.

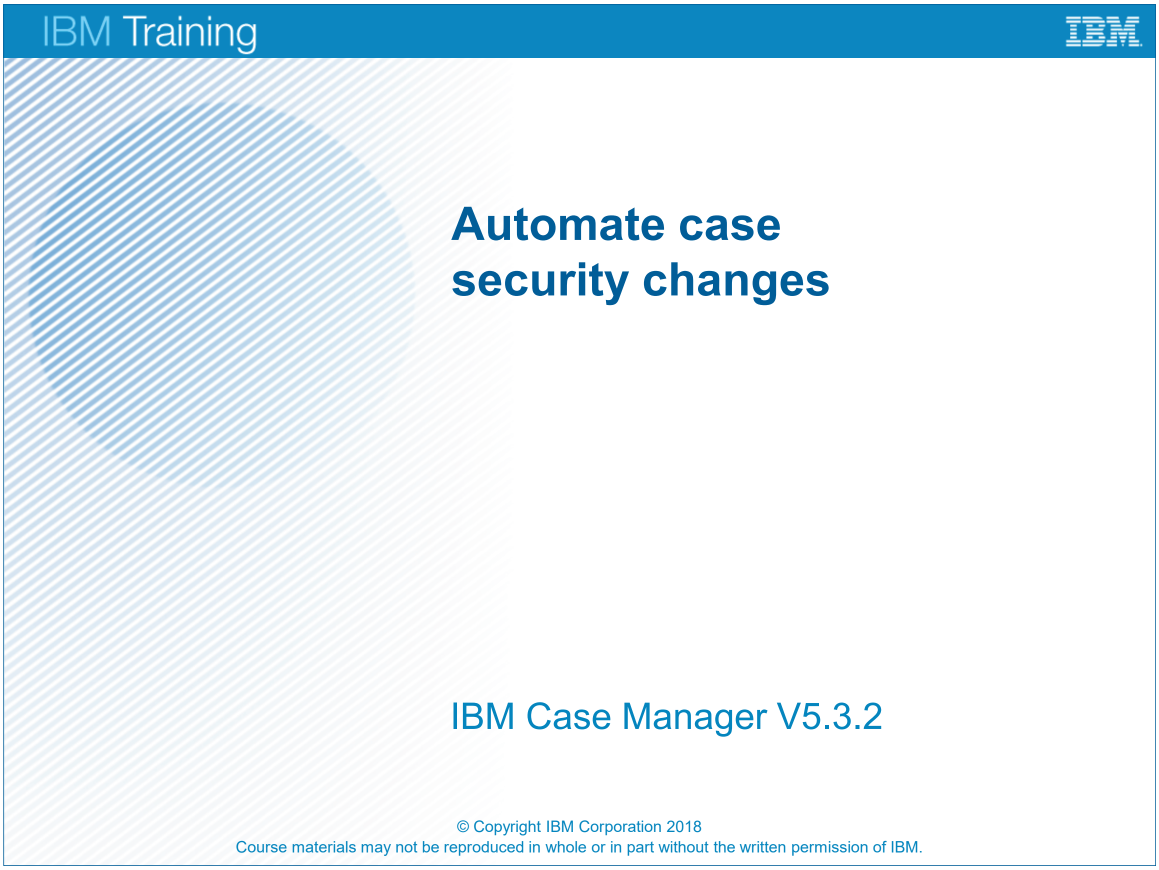
   a. Security configuration – correct answer

   c. Solution definition – correct answer

5. How do you export and import altered solution objects, such as case-type folders, to a new environment?

   d. You do not – correct answer

Appendix A. Automate case security changes

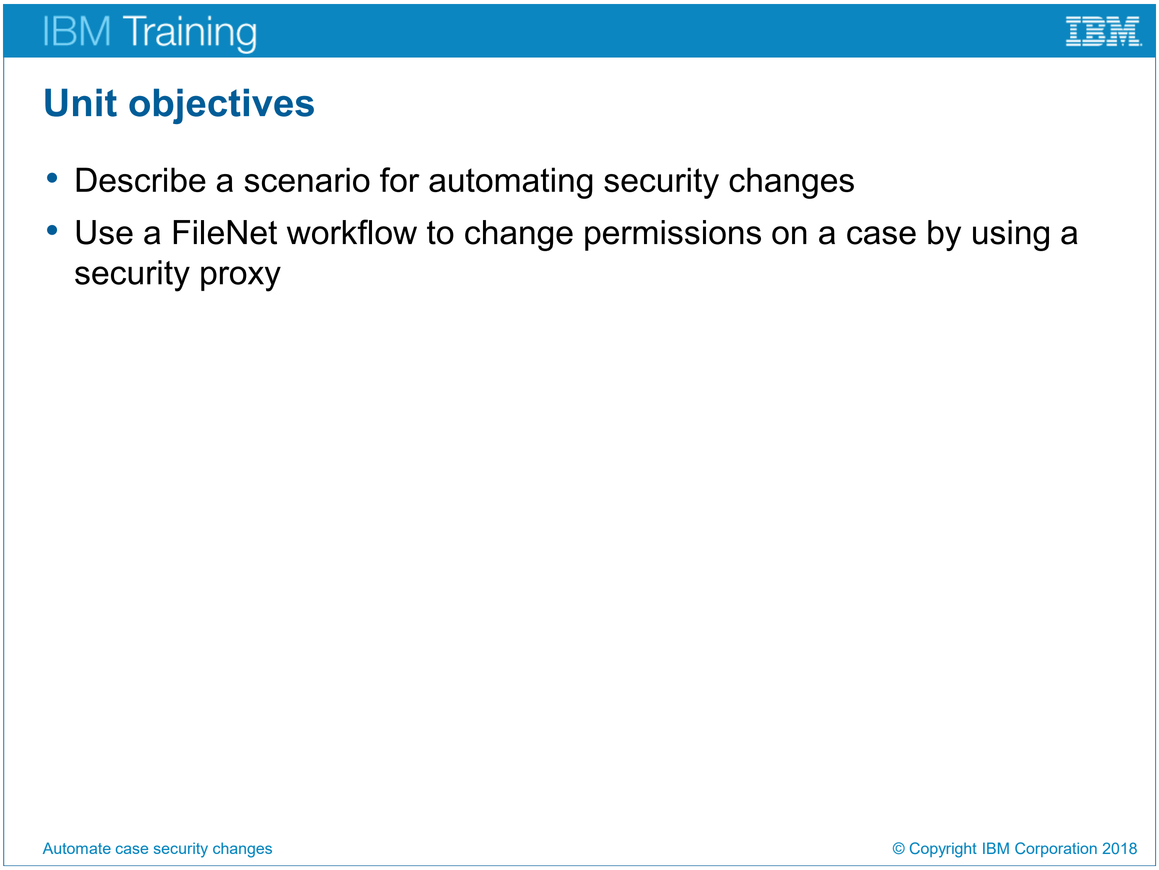


IBM Training

IBM

Automate case security changes

IBM Case Manager V5.3.2



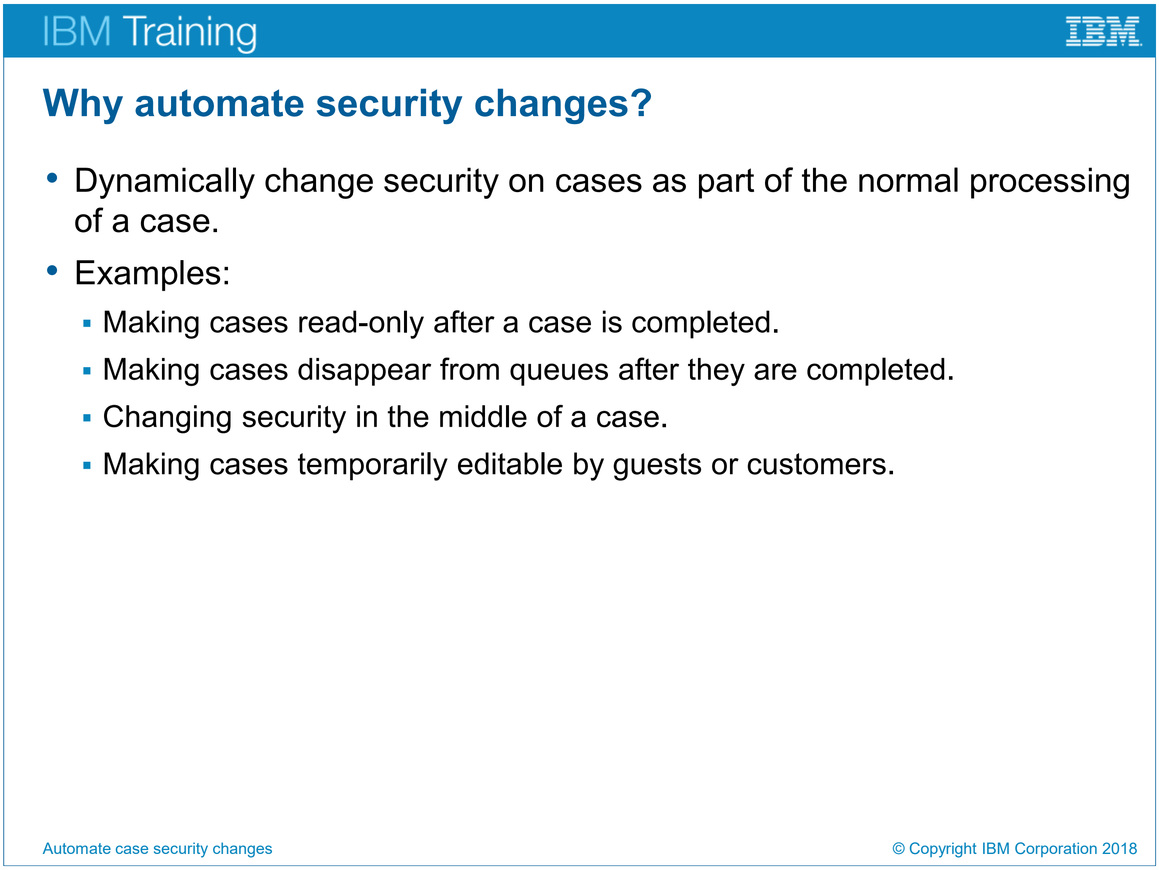
IBM Training

Unit objectives

- Describe a scenario for automating security changes
- Use a FileNet workflow to change permissions on a case by using a security proxy

Automate case security changes

Unit objectives



IBM Training

Why automate security changes?

- Dynamically change security on cases as part of the normal processing of a case.
- Examples:
  - Making cases read-only after a case is completed.
  - Making cases disappear from queues after they are completed.
  - Changing security in the middle of a case.
  - Making cases temporarily editable by guests or customers.

Automate case security changes

Why automate security changes?

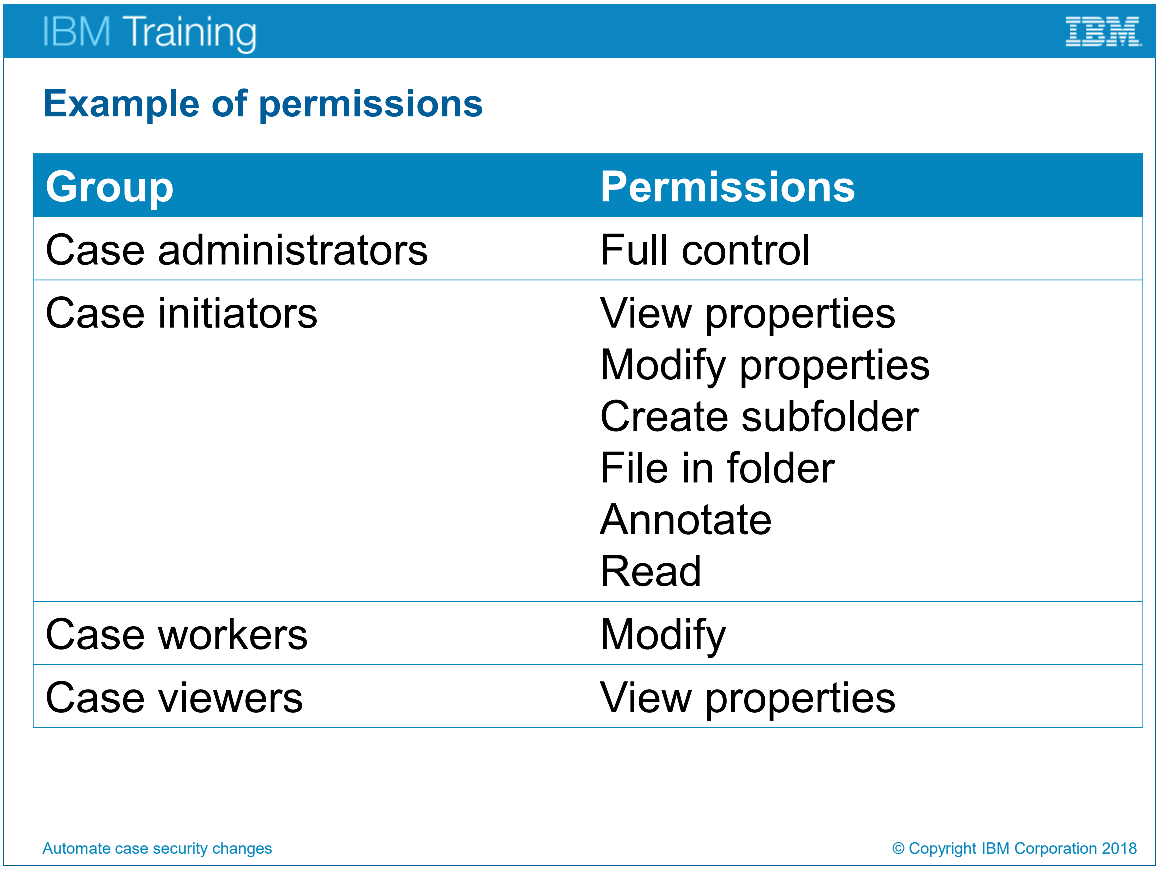
You might automate security changes when you want security on cases to dynamically change as part of the normal processing of a case. You want to allow updates during the working life of a case, but after a case is completed, you want to prevent users from updating case properties.

This scenario provides an in-depth analysis of a business use case.

A company needs to prevent caseworkers from altering case data after the case is completed. During the working period of a case, caseworkers can update the case, add documents to the case and complete tasks. When the case is completed, the caseworkers have view-only rights. You can achieve these effects by using a security proxy and a FileNet workflow.

Use this checklist to set up a security proxy to satisfy the scenario objectives.

- In the security configuration, set all permissions to view only, except for the case initiator. This behavior is the default for the case.
- Create a security proxy that provides update permissions.
- Create another security proxy that provides a smaller set of permissions.
- Assign the case folder class a default value for the parent proxy OVP.
- Use a FileNet workflow step to change the OVP value on the case.



IBM Training

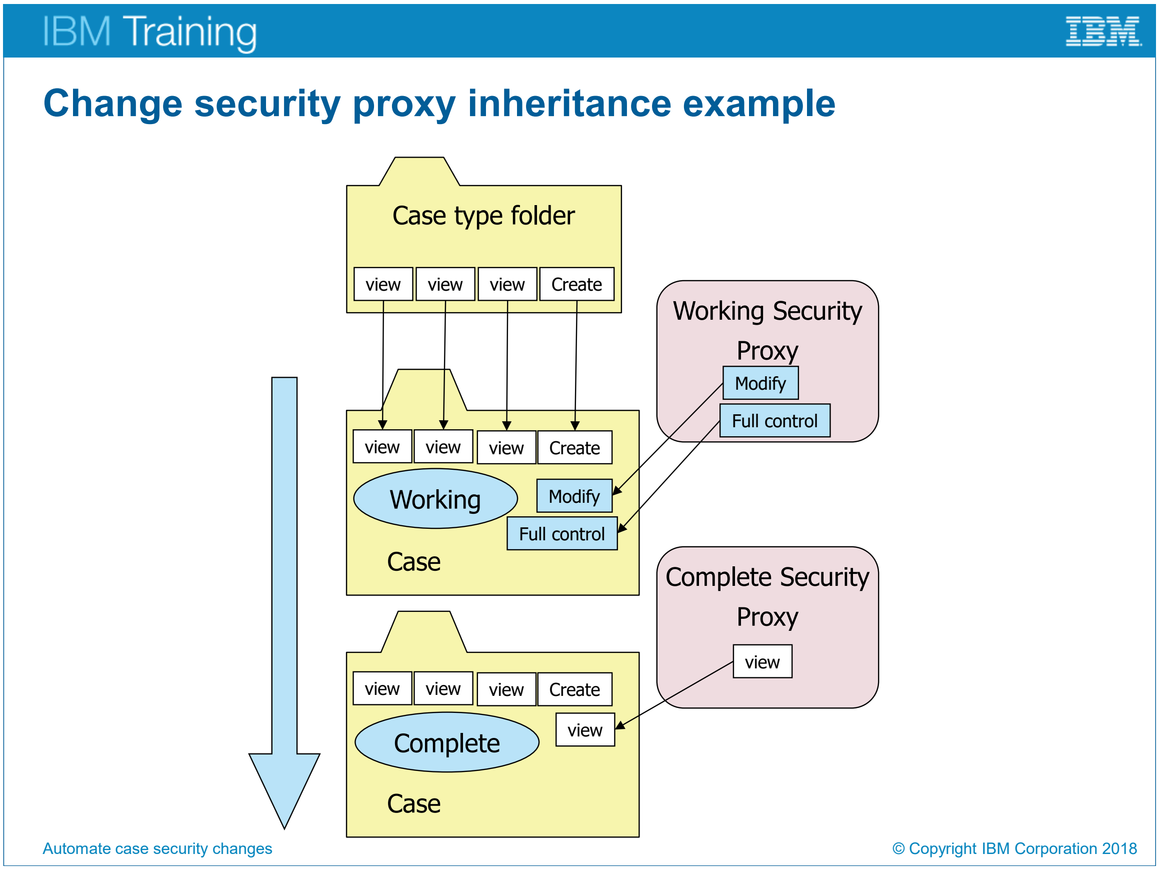
Example of permissions

Group	Permissions
Case administrators	Full control
Case initiators	View properties Modify properties Create subfolder File in folder Annotate Read
Case workers	Modify
Case viewers	View properties

Automate case security changes

Example of permissions

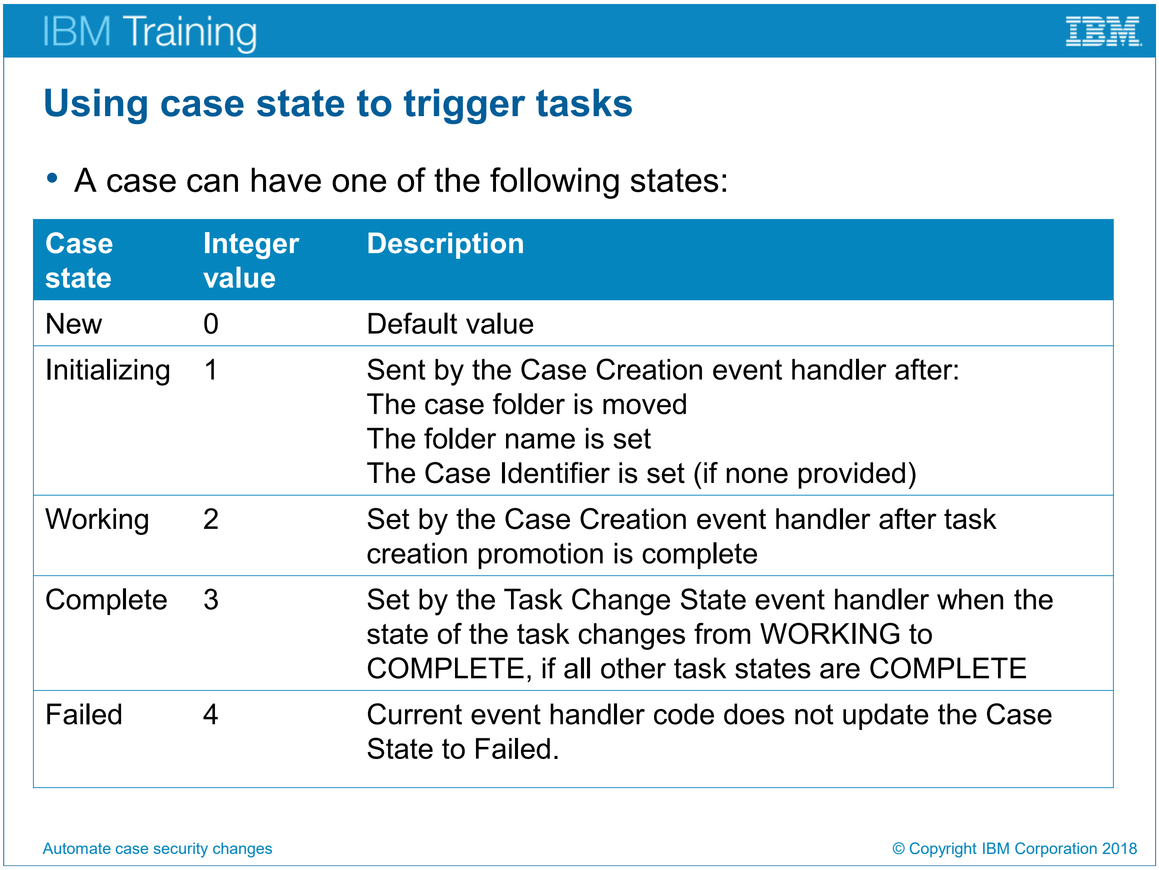
When a security proxy provides case permissions, you must specify inheritable permissions on the security proxy to satisfy the access requirements of each role. On the security proxy, you must set permissions to be applied to all children, but not this object.



Change security proxy inheritance example

The graphic shows an example of how automation changes security on a case.

Initially, all roles have view-only access except receptionists because they need permissions to create cases. The case inherits security from the case type folder. When the case is in the working state, permissions are inherited from the Working Security Proxy. When the case is complete, permissions are inherited from the Complete Security Proxy. You can provide view access to users who were not originally part of the case after the case is complete. Alternately, you can remove the security proxy and allow the permissions from case type folder to control case access.



IBM Training

Using case state to trigger tasks

- A case can have one of the following states:

Case state	Integer value	Description
New	0	Default value
Initializing	1	Sent by the Case Creation event handler after: The case folder is moved The folder name is set The Case Identifier is set (if none provided)
Working	2	Set by the Case Creation event handler after task creation promotion is complete
Complete	3	Set by the Task Change State event handler when the state of the task changes from WORKING to COMPLETE, if all other task states are COMPLETE
Failed	4	Current event handler code does not update the Case State to Failed.

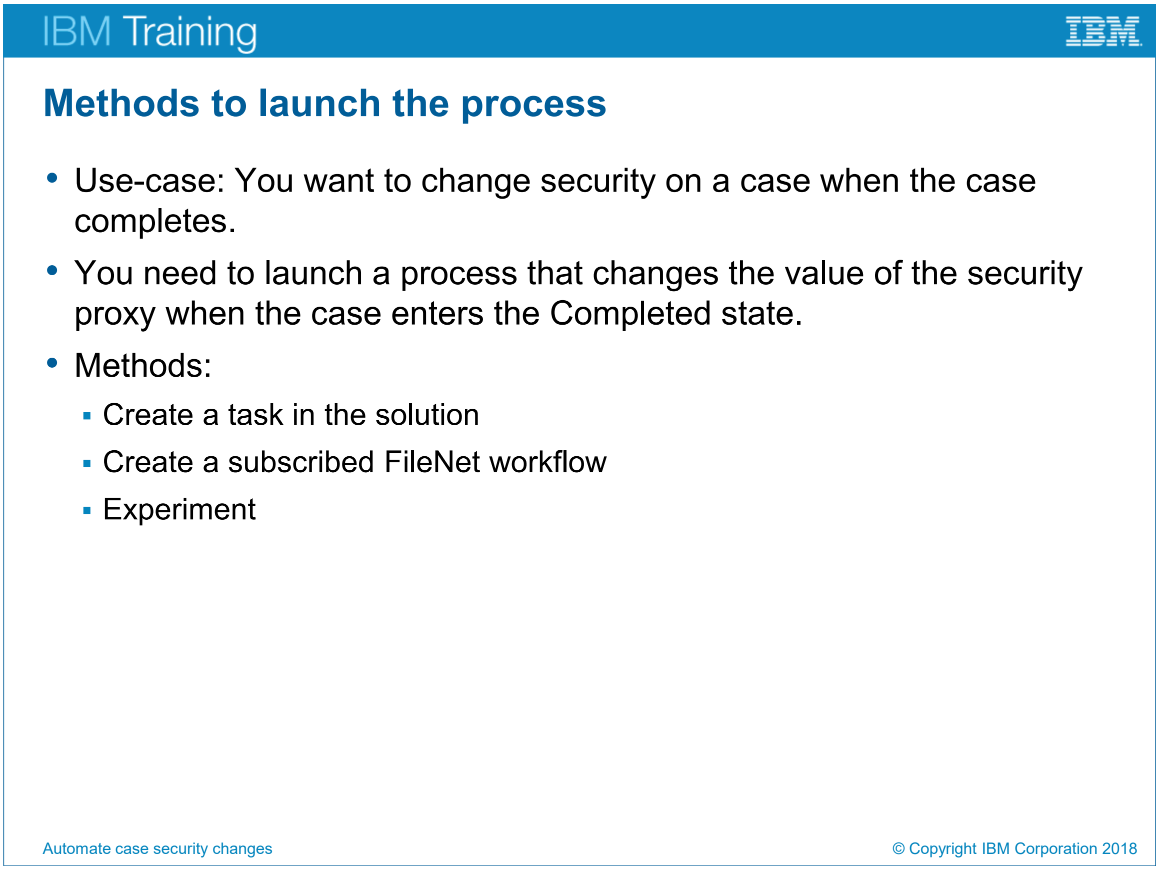
Automate case security changes

Using case state to trigger tasks

To use the case state as a trigger for changing security, you must understand the case states and how they are organized in the system.

The case state is a property of the case folder class. You can use the case state property to trigger a task. The symbolic name is cmAcmCaseState.

A case enters the completed state when all required tasks are complete. A case cannot complete if any required task is not completed or if a started task is not completed or cancelled. A case can be moved back into the Working state if a new task is started on a case. When a task is started, it becomes required.



IBM Training

Methods to launch the process

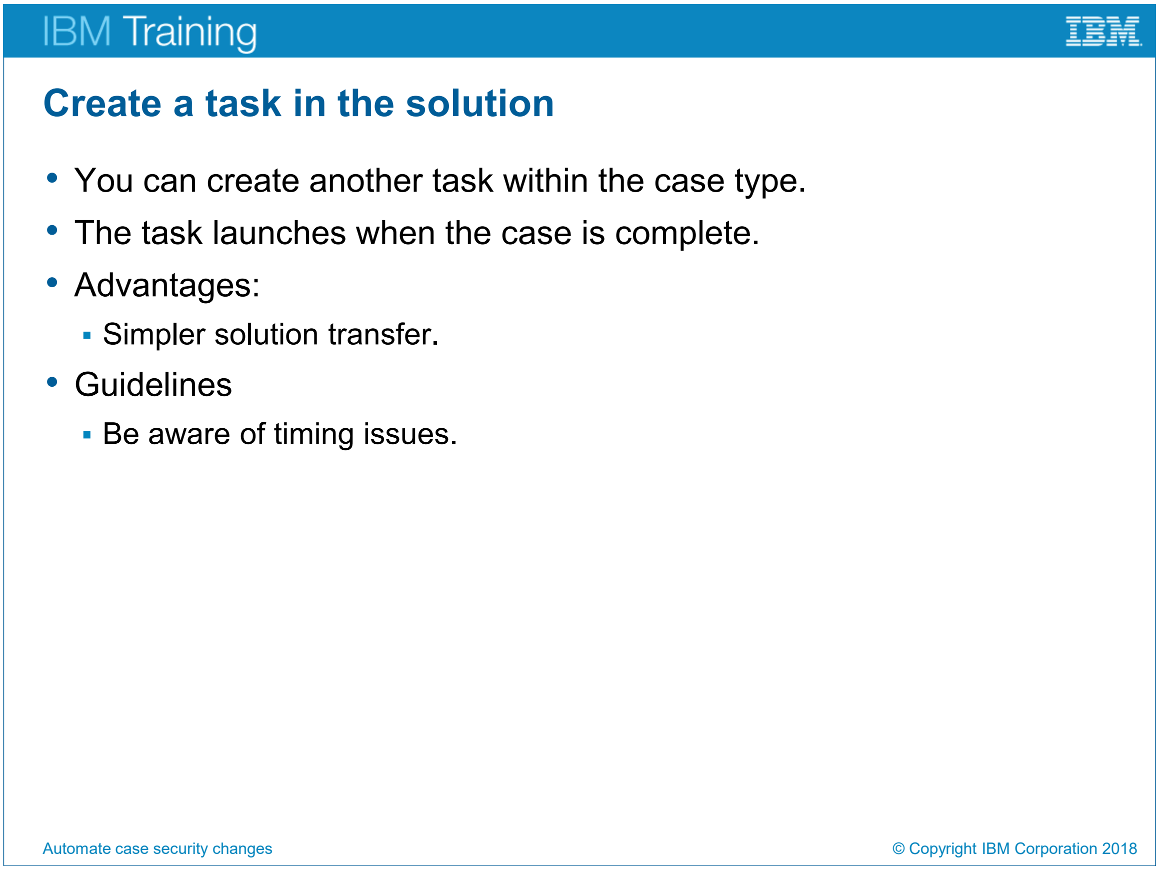
- Use-case: You want to change security on a case when the case completes.
- You need to launch a process that changes the value of the security proxy when the case enters the Completed state.
- Methods:
  - Create a task in the solution
  - Create a subscribed FileNet workflow
  - Experiment

Automate case security changes

Methods to launch the process

You need to launch a process that changes the value of the security proxy when the case enters the state, Completed. More than one method exists to accomplish this goal.

- Case type: One way is to create a task in the solution. This method involves creating a task within the case type that launches when the case completes.
- Separate FileNet workflow: Another way is to create an external task. This method involves creating a separate FileNet workflow that is launched by a subscribed event on the deployed case type class.
- Other methods: You can experiment with other methods as well, such as working the property change within a case task and manual launch methods.



IBM Training

Create a task in the solution

- You can create another task within the case type.
- The task launches when the case is complete.
- Advantages:
  - Simpler solution transfer.
- Guidelines
  - Be aware of timing issues.

Automate case security changes

© Copyright IBM Corporation 2018

Create a task in the solution

You can create another task within the case type. The task launches when the case is complete.

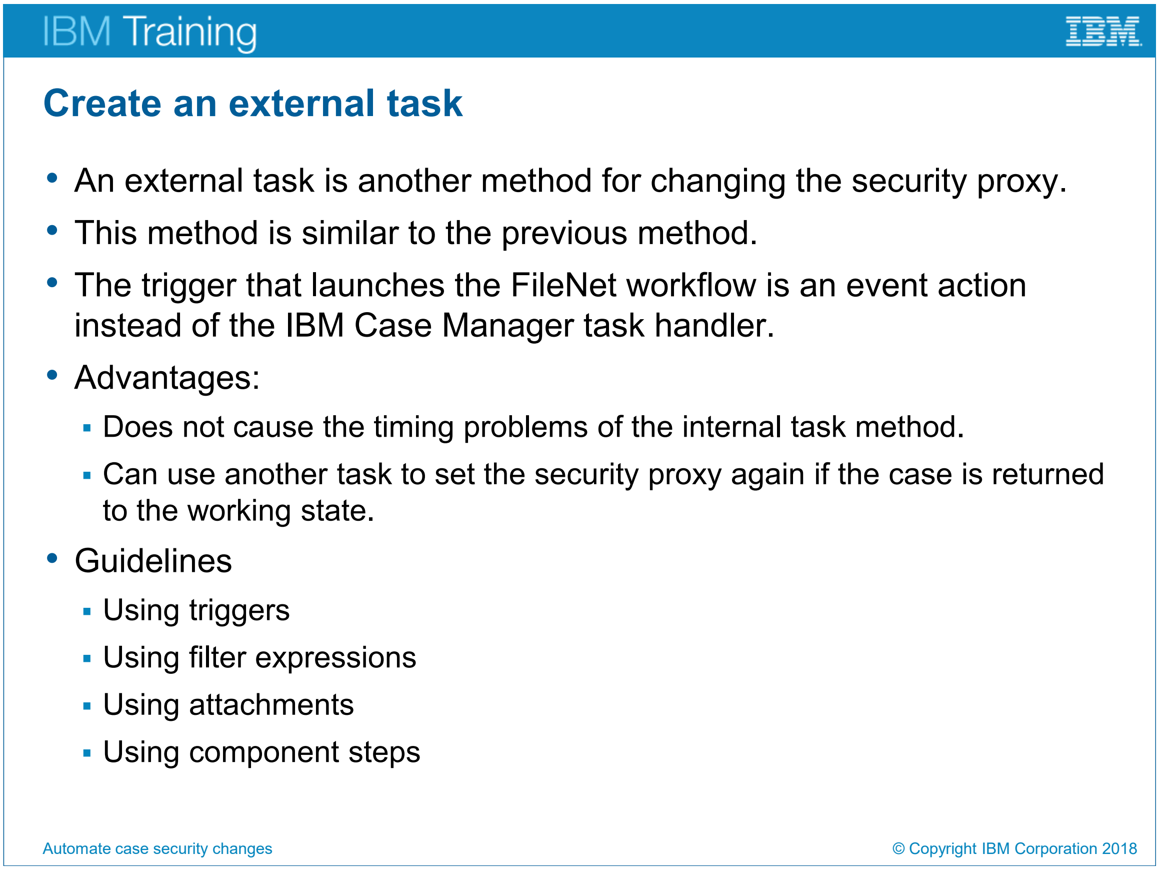
Be aware of timing issues. When a task starts, it becomes required. If any required tasks are running, the case cannot be in a Complete state. Starting a task within a case type when the case is completed can work, but it can be sensitive to timing issues.

- Tasks do not start the instant that their preconditions are met. The state changes are queued for execution when their preconditions are met.
- If the task starts too quickly, it can cause other systems, such as reporting tools, to fail. For example, Case Analyzer can interpret a single case as multiple case creation events.

The main advantage for using a task for this purpose is that using FileNet workflows that are part of the solution simplifies the migration process.

Use the following guidelines when setting up this type of automation:

- Reuse the acmCaseState property to use it as a precondition.
- Use attachments for the security proxy and the case folder.
- Use the CE_Operation: getObjectFromPath to obtain values for the case folder and security proxy attachment fields.
- Use the CE_Operation: setObjectProperty to change the value of the OVP on the case folder.
- Use an Optional task. If the task is Required, the case state remains in the Working state.
- Add a delay step to prevent the task from starting too early.



IBM Training

Create an external task

- An external task is another method for changing the security proxy.
- This method is similar to the previous method.
- The trigger that launches the FileNet workflow is an event action instead of the IBM Case Manager task handler.
- Advantages:
  - Does not cause the timing problems of the internal task method.
  - Can use another task to set the security proxy again if the case is returned to the working state.
- Guidelines
  - Using triggers
  - Using filter expressions
  - Using attachments
  - Using component steps

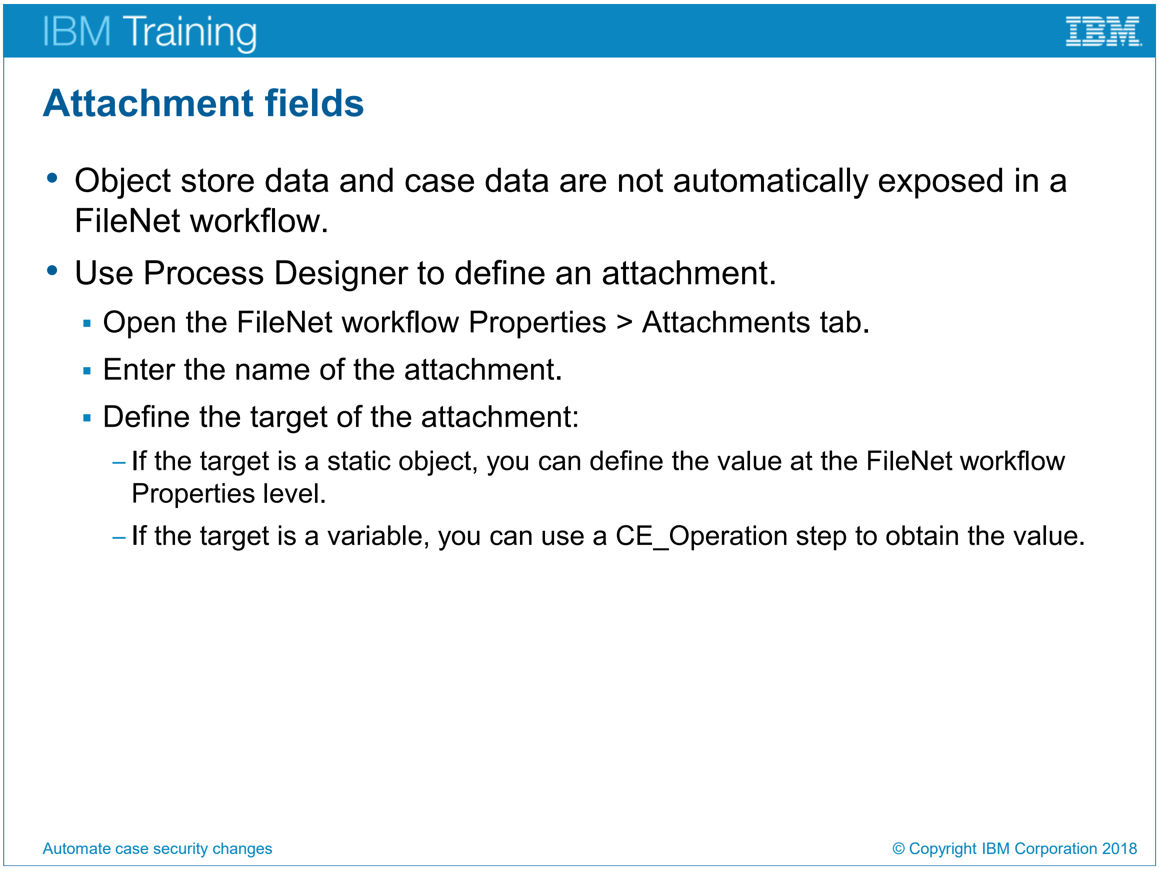
Automate case security changes

© Copyright IBM Corporation 2018

Create an external task

Use the following guidelines when setting up this type of automation:

- Use an update event trigger on the deployed case type folder class.
- Use a filter expression to limit the trigger, for example: acmCaseState = 3.
- Use attachments for the security proxy and the case folder.
- Use the initiating attachment to obtain the value of the folder.
- Use the CE_Operation: getObjectFromPath to obtain the value for the security proxy attachment field.
- Use the CE_Operation: setObjectProperty to change the value of the OVP on the case folder.



IBM Training

Attachment fields

- Object store data and case data are not automatically exposed in a FileNet workflow.
- Use Process Designer to define an attachment.
  - Open the FileNet workflow Properties > Attachments tab.
  - Enter the name of the attachment.
  - Define the target of the attachment:
    - If the target is a static object, you can define the value at the FileNet workflow Properties level.
    - If the target is a variable, you can use a CE_Operation step to obtain the value.

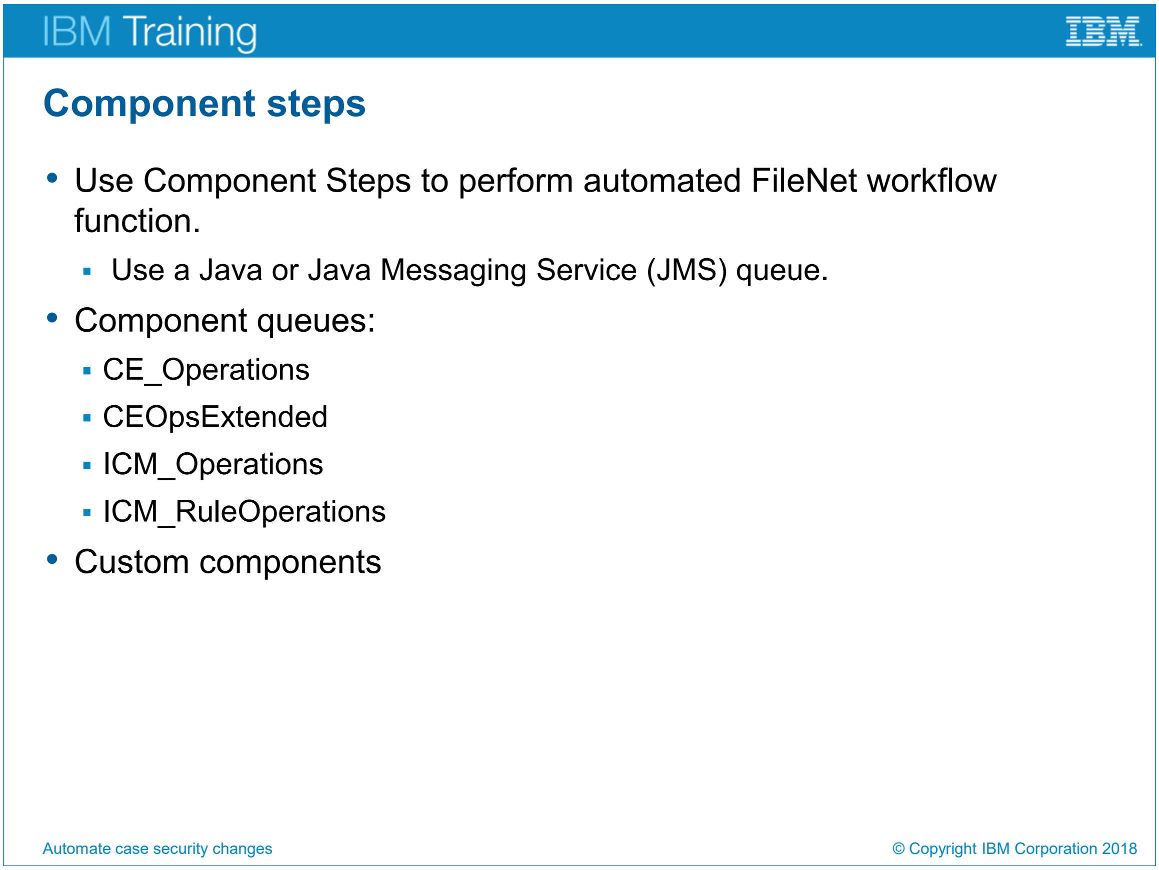
Automate case security changes

© Copyright IBM Corporation 2018

Attachment fields

An attachment is a link (a pointer) to information that a participant uses to complete a step in a FileNet workflow.

The specific item that an attachment links to is referred to as a target. The most common target is a document that is located in an object store. In addition, document arrays, custom objects, stored searches, folders, web addresses, or files that are on a shared disk can also be targets of an attachment.



IBM Training

Component steps

- Use Component Steps to perform automated FileNet workflow function.
  - Use a Java or Java Messaging Service (JMS) queue.
- Component queues:
  - CE_Operations
  - CEOpsExtended
  - ICM_Operations
  - ICM_RuleOperations
- Custom components

Automate case security changes

© Copyright IBM Corporation 2018

Component steps

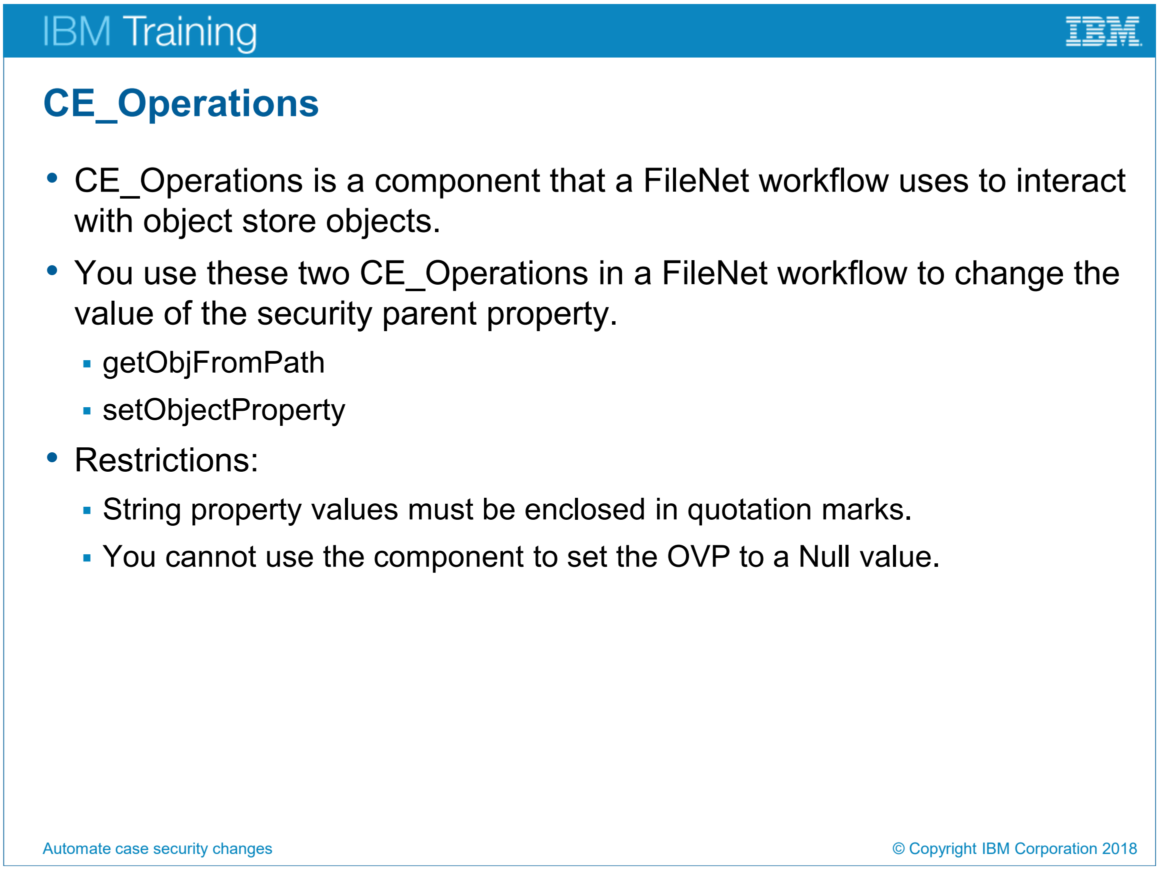
In Process Designer, you define the Component Steps that run an automated FileNet workflow functions by using a Java or Java Messaging Service (JMS) queue.

Component queues must be defined in Administration Console for Content Platform Engine in order for you to use them in a FileNet workflow. Each component queue has one or more functions that you can use to run FileNet workflow tasks.

In addition to the included component queues, you can create your own components. For more information about components, consider taking the following course:

F243G: IBM Case Foundation 5.2.1: External Communication

https://www-03.ibm.com/services/learning/ites.wss/zz-en?pageType=course_description&cc=&courseCode=F243G



IBM Training

CE_Operations

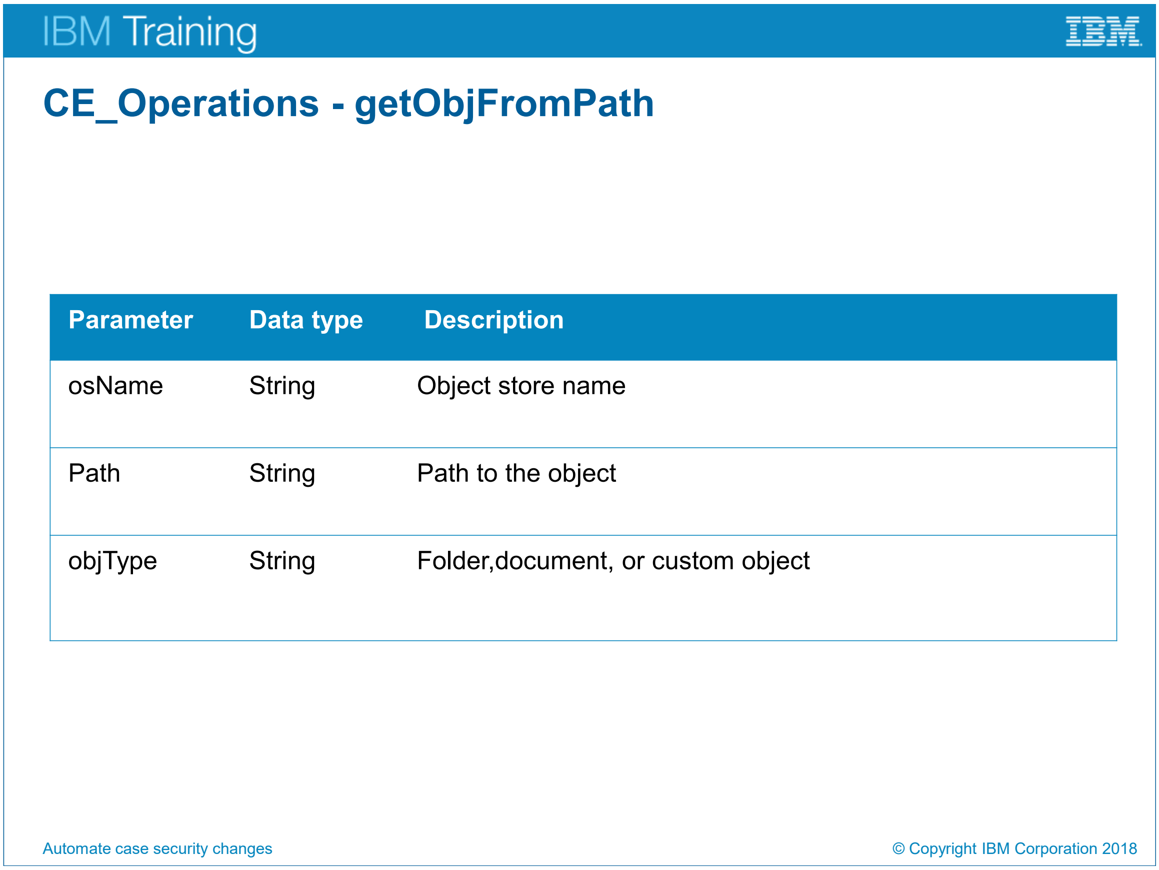
- CE_Operations is a component that a FileNet workflow uses to interact with object store objects.
- You use these two CE_Operations in a FileNet workflow to change the value of the security parent property.
  - getObjFromPath
  - setObjectProperty
- Restrictions:
  - String property values must be enclosed in quotation marks.
  - You cannot use the component to set the OVP to a Null value.

Automate case security changes

© Copyright IBM Corporation 2018

CE_Operations

Use CE_Operations functions in a FileNet workflow to change the value of the security parent property.



IBM Training

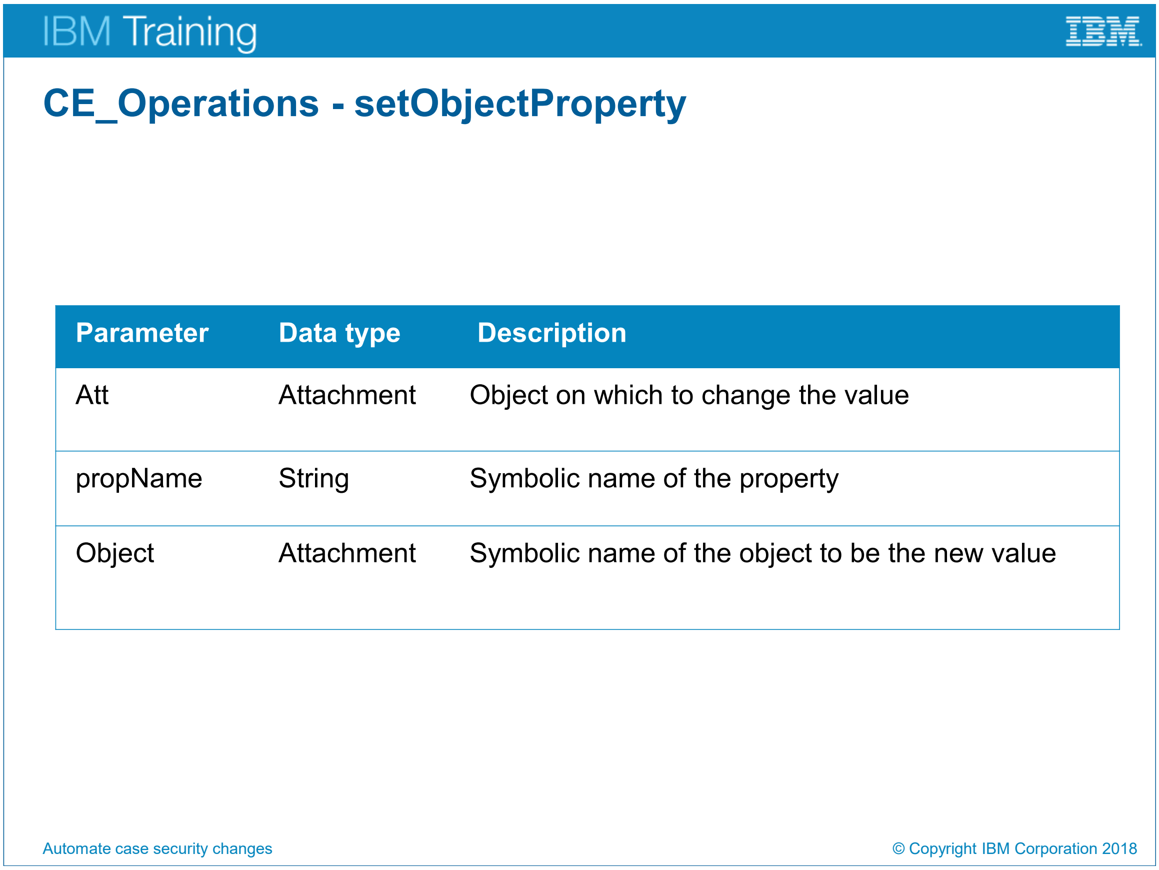
CE_Operations - getObjFromPath

Parameter	Data type	Description
osName	String	Object store name
Path	String	Path to the object
objType	String	Folder,document, or custom object

Automate case security changes

CE_Operations - getObjFromPath

This function gets an object (custom object, folder or document) from a specified repository using a specified path.



IBM Training

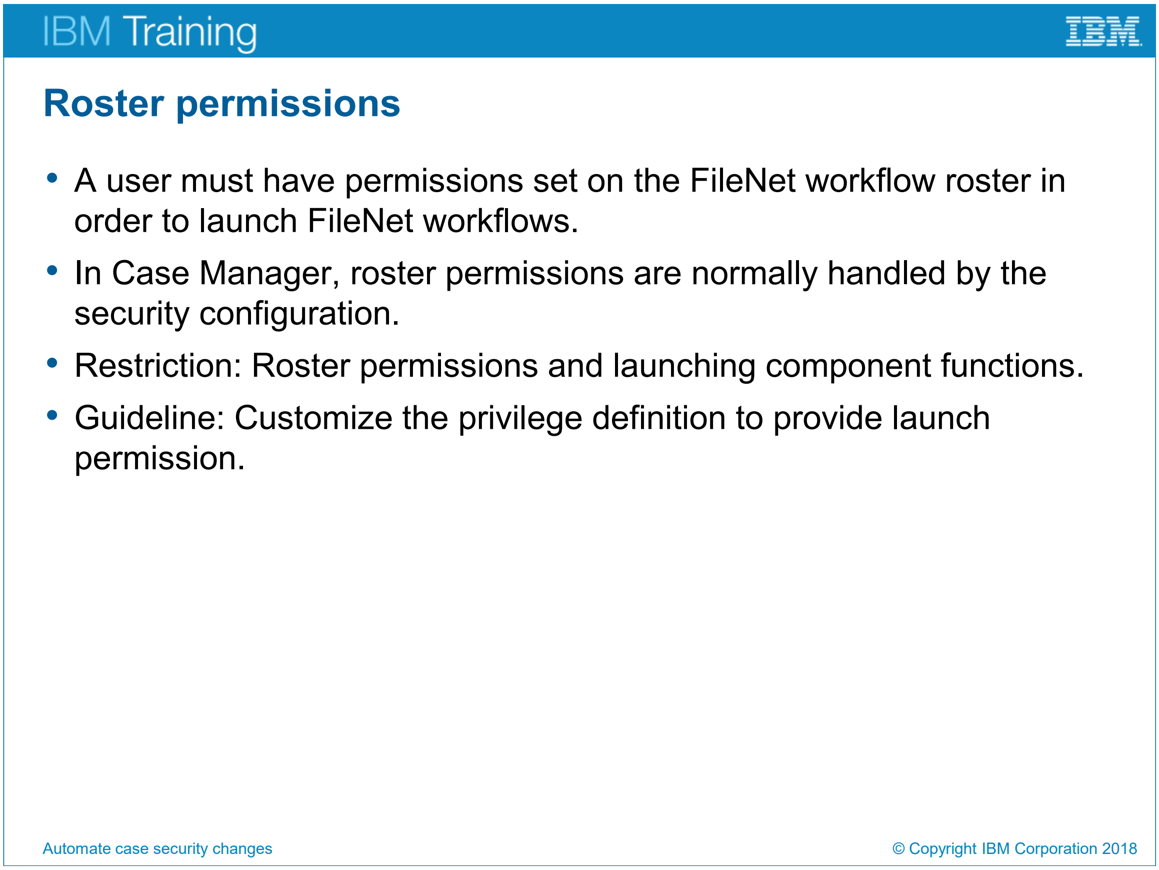
CE_Operations - setObjectProperty

Parameter	Data type	Description
Att	Attachment	Object on which to change the value
propName	String	Symbolic name of the property
Object	Attachment	Symbolic name of the object to be the new value

Automate case security changes

CE_Operations - setObjectProperty

This function sets the object value of an object-valued property.



IBM Training

Roster permissions

- A user must have permissions set on the FileNet workflow roster in order to launch FileNet workflows.
- In Case Manager, roster permissions are normally handled by the security configuration.
- Restriction: Roster permissions and launching component functions.
- Guideline: Customize the privilege definition to provide launch permission.

Automate case security changes

© Copyright IBM Corporation 2018

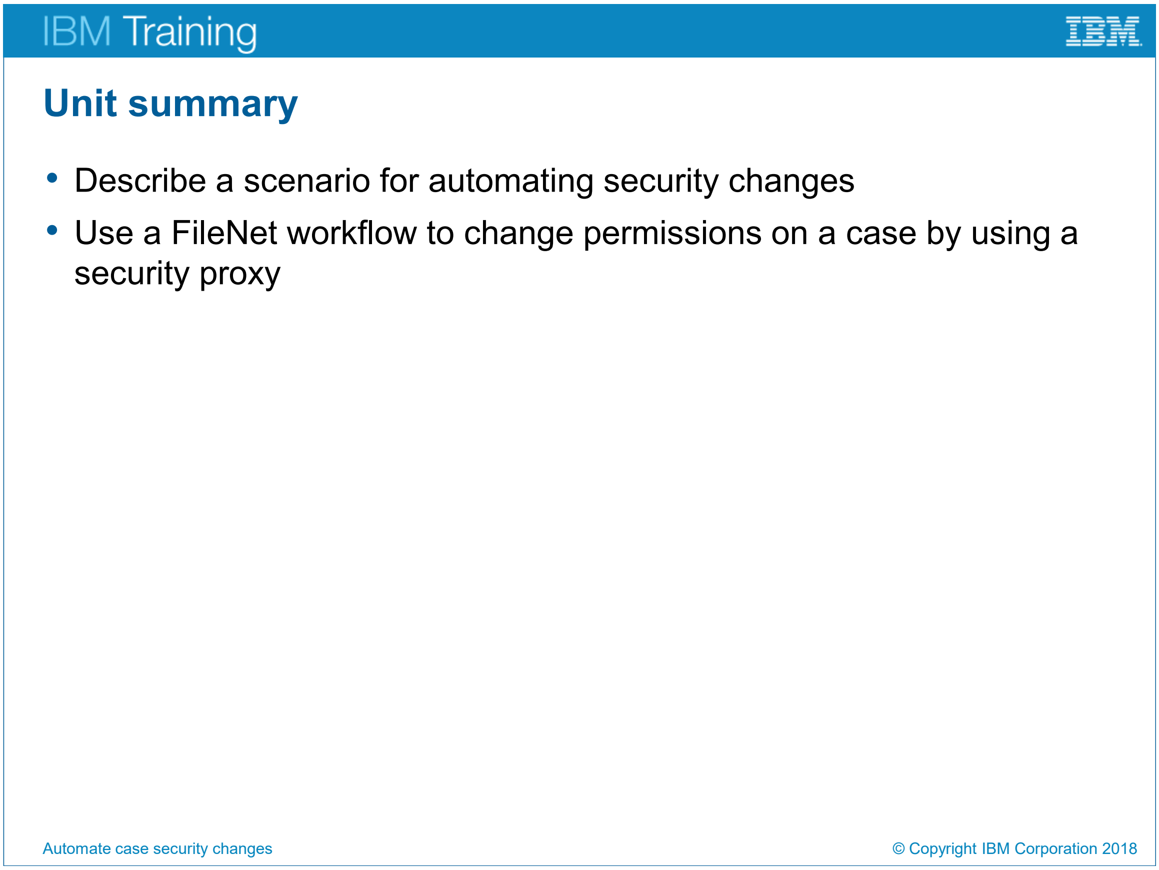
Roster permissions

If you use a security proxy object to provide permissions to users you must ensure that roles have sufficient permissions to launch FileNet workflows. Permissions granted by the security proxy do not extend to FileNet workflow processing. You must ensure that anyone who completes work items has sufficient permission to process FileNet workflow items.

A roster is a database structure to track work items. Each FileNet workflow application uses one FileNet workflow roster. A roster contains references to all running FileNet workflows and work items for the application. Rosters are used for finding work items in Process Administrator. A user must have permission to launch FileNet workflows on the roster to launch FileNet workflows.

Be aware of the following restriction: A task in Case Manager is a FileNet workflow. A FileNet workflow is launched by using the same credentials as the person who completed the previous step. If that person does not have permission to launch FileNet workflows on the FileNet workflow roster, then the FileNet workflow fails to launch.

One useful guideline is that you can customize the privilege definition file to give users permission to launch FileNet workflows. You can use the custom privilege definition when you create the Security Configuration. Security configuration affects many different areas of security, including FileNet workflow security. Extra permissions are needed to initiate a case type, so users who can launch FileNet workflows cannot create cases without that permission.



IBM Training

Unit summary

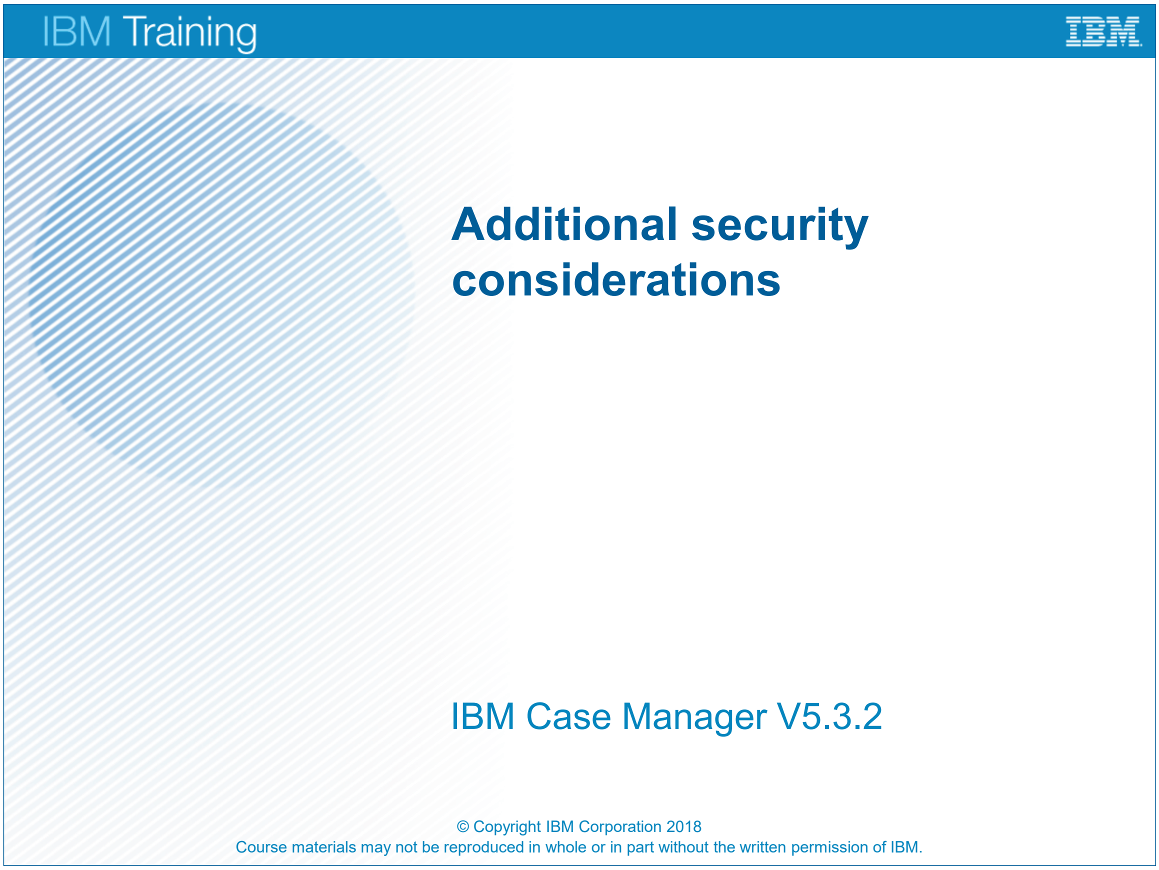
- Describe a scenario for automating security changes
- Use a FileNet workflow to change permissions on a case by using a security proxy

Automate case security changes

© Copyright IBM Corporation 2018

Unit summary

Appendix B. Additional security considerations



IBM Training

Additional security considerations

IBM Case Manager V5.3.2

IBM Training

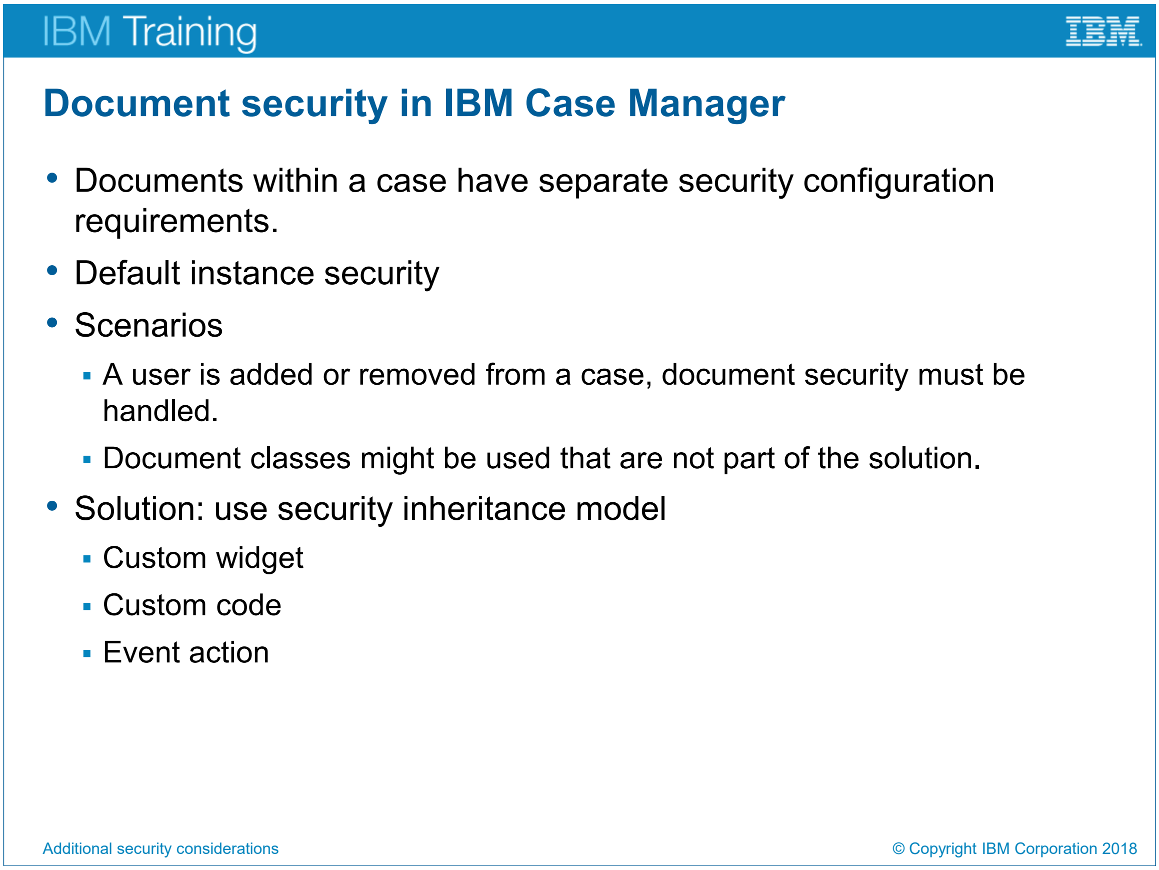
Unit objectives

- Analyze scenarios that require specific security customizations

Additional security considerations

© Copyright IBM Corporation 2018

Unit objectives



IBM Training

Document security in IBM Case Manager

- Documents within a case have separate security configuration requirements.
- Default instance security
- Scenarios
  - A user is added or removed from a case, document security must be handled.
  - Document classes might be used that are not part of the solution.
- Solution: use security inheritance model
  - Custom widget
  - Custom code
  - Event action

Additional security considerations

© Copyright IBM Corporation 2018

Document security in IBM Case Manager

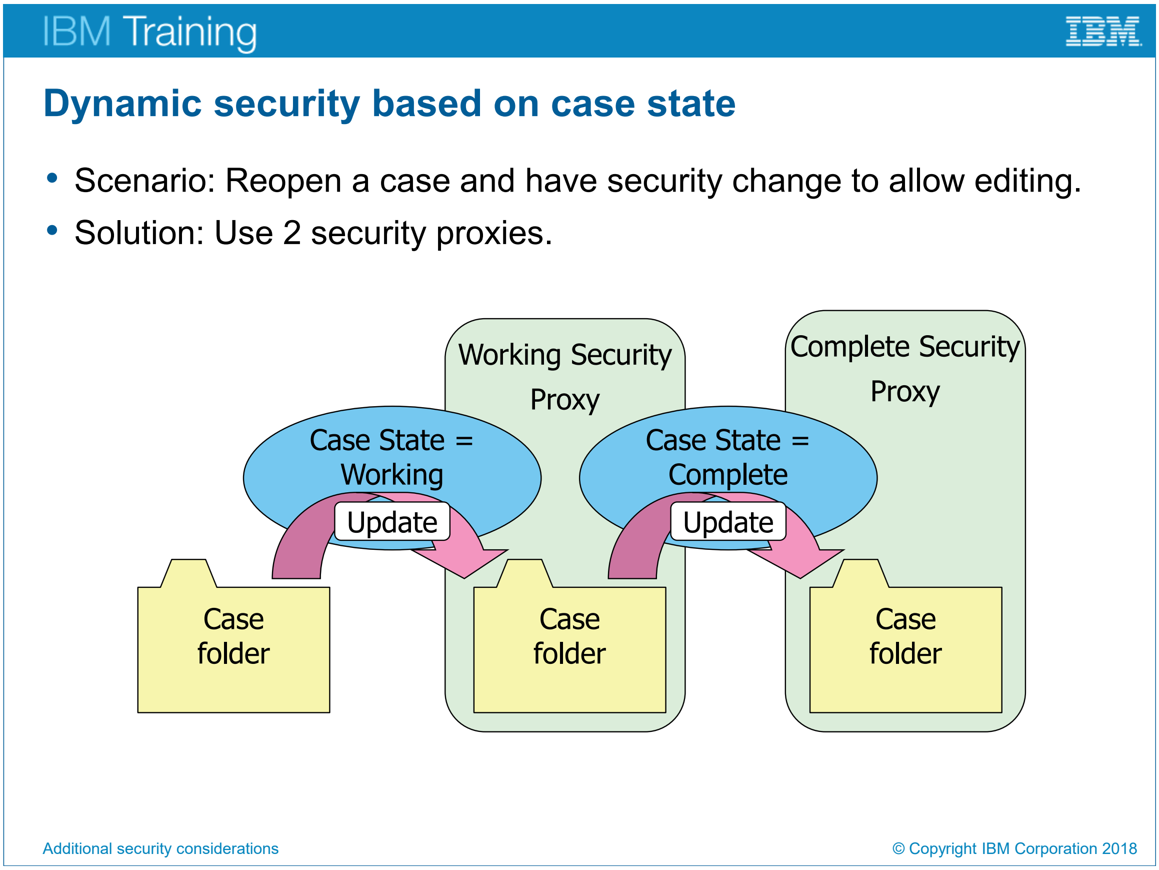
Case Manager handles document security with the standard default instance security model controlled by document subclasses. In most scenarios, a user who has access to a case also has access to document classes.

Default instance security does not always suffice for the following reasons:

- The solution designer cannot predict all of the document classes that might be used in a case.
- Adjusting document security individually is not dynamic. For example, if the user is later removed from the case, the document security is unchanged.

One solution to these issues is to configure the security of the documents to inherit security settings from the case folder or subfolder. You can use the following methods:

- Use a custom widget to set the value of the parent folder when the document is added.
- Create custom code that works directly with the Content Platform Engine APIs to automate the setting to inherit security from the folder.
- Use an event action to set the security inheritance to the parent folder.



IBM Training

Dynamic security based on case state

- Scenario: Reopen a case and have security change to allow editing.
- Solution: Use 2 security proxies.

Additional security considerations

© Copyright IBM Corporation 2018

Dynamic security based on case state

When a case completes, caseworkers have read-only access to case data. If a case administrator decides to reopen the case, then the case security must be changed back to allow caseworkers to access and update it.

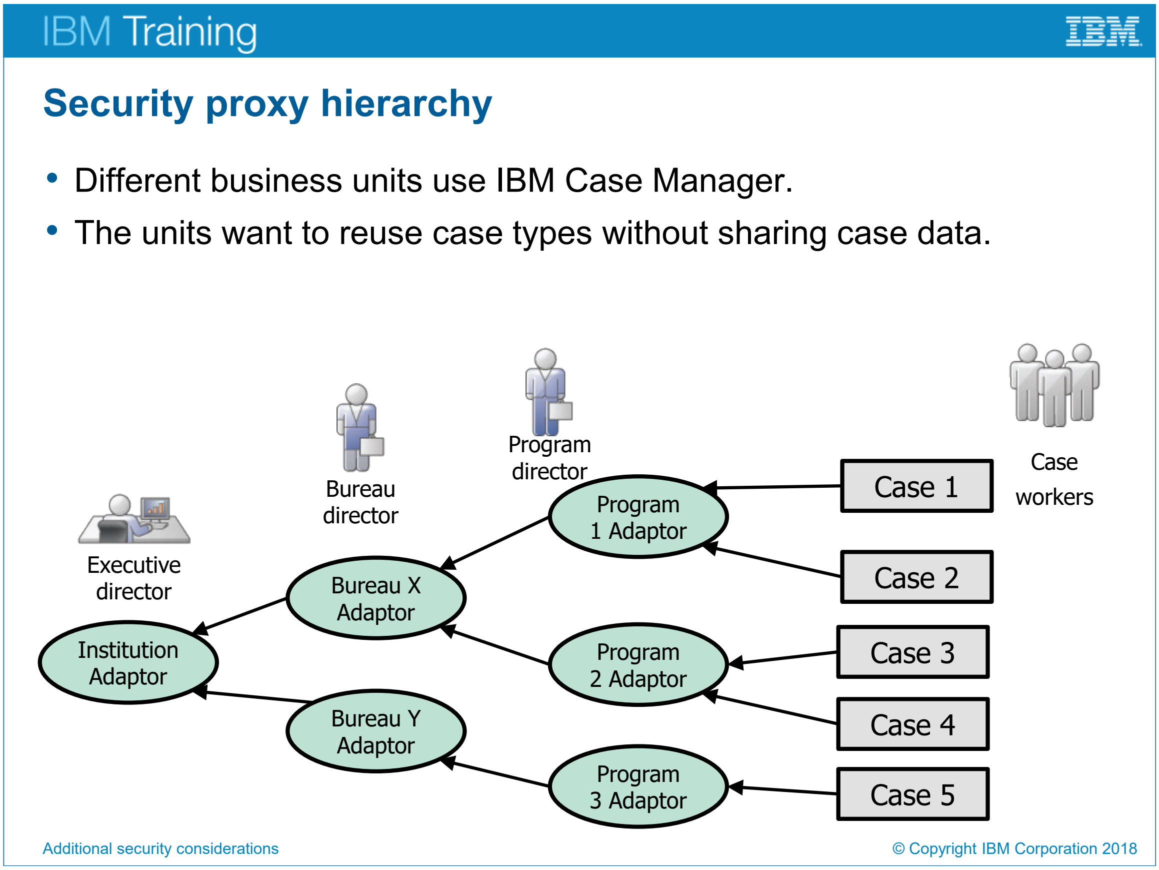
Use an event subscription to set the object-valued property (OVP) value on the case folder back to the Working value when the case state is Working.

Set up no security (or View and Initiate only) on cases by default with the Security Configuration.

Set up two event subscriptions, one to change the OVP when the case is Working and one to change the OVP when the case is Complete.

Use the Update event on the case type folder class.

Use filter expressions to limit the actions to when the case is Working and Complete.



IBM Training

Security proxy hierarchy

- Different business units use IBM Case Manager.
- The units want to reuse case types without sharing case data.

Executive director

Bureau director

Program director

Case workers

Institution Adaptor

Bureau X Adaptor

Bureau Y Adaptor

Program 1 Adaptor

Program 2 Adaptor

Program 3 Adaptor

Case 1

Case 2

Case 3

Case 4

Case 5

Additional security considerations

© Copyright IBM Corporation 2018

Security proxy hierarchy

In a large corporation, several different business units want to use IBM Case Manager to handle their line-of-business needs. The types of cases are the same. You want to reuse the same case types across the enterprise. However, you do not want the different business units to have access to one another’s cases. You can use a security proxy hierarchy to secure the cases from other business units.

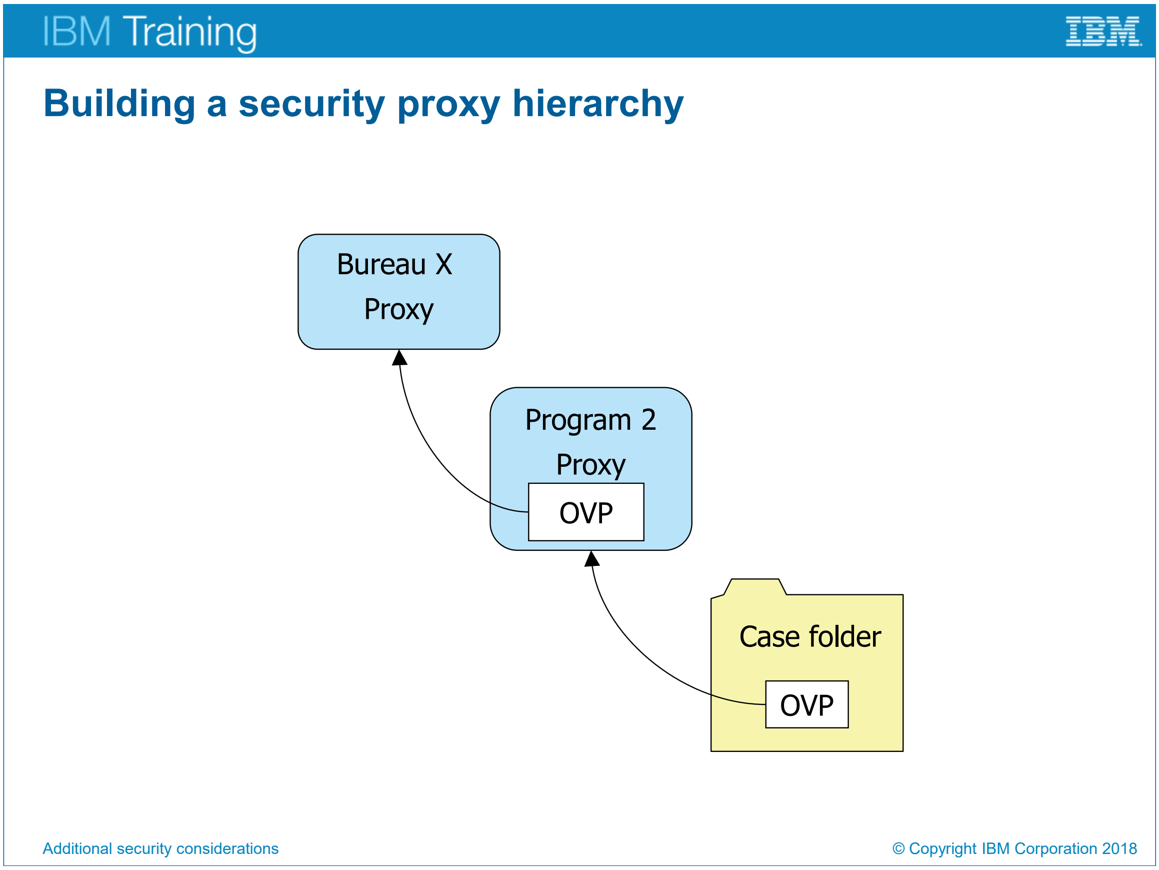
You can use multiple security proxies on the same object, or even construct security proxy hierarchies if your solution requires it.

A security proxy hierarchy is a set of security proxies that are set up to duplicate the corporate structure. Security proxies can serve as both parents and children for other security proxies. When you assign a security proxy to a case folder, it inherits permissions from that security proxy and all of the permissions that are inherited from its parent proxies.

Using a security proxy hierarchy provides a way to manage security between business units that use the same case type. Therefore, you can design a case type one time and reuse it across multiple business units. The security hierarchy ensures that each business unit can access only cases within that unit. If a business unit moves or is reassigned, you can manage the security proxy hierarchy to reflect the new corporate arrangement, and so retain security on cases.

Use automation to assign the security proxy when the case is added. For example, you can set the security parent value by default, or you can use the case folder creation event to trigger the proxy assignment.

For example, a corporation consolidates two bureaus into one. All of the cases that Bureau X was responsible for are now the responsibility of Bureau Y. Both bureaus use the same case type, but the cases are secured by using a security proxy hierarchy. By editing the security proxy hierarchy, you can move Program 2 under Bureau Y and instantly change the functional security on all of the associated cases.



IBM Training

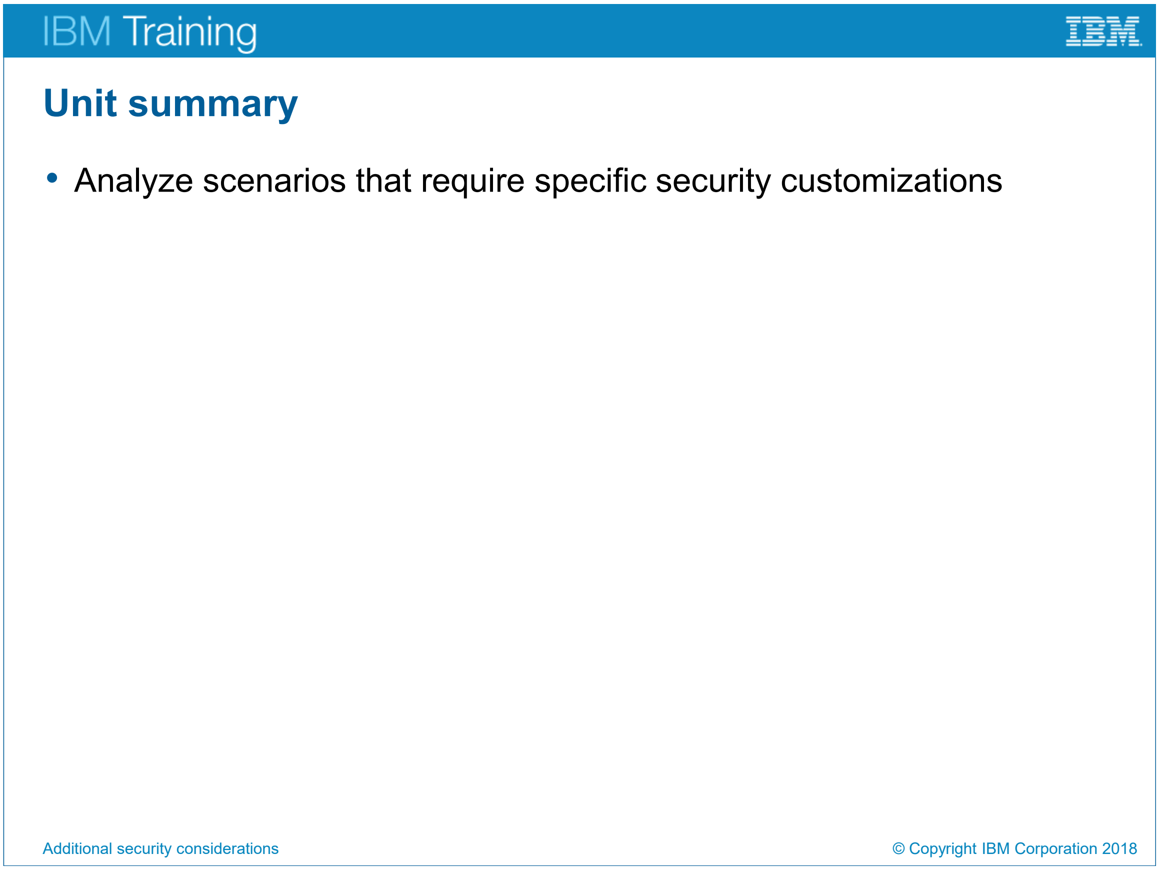
Building a security proxy hierarchy

Additional security considerations

© Copyright IBM Corporation 2018

Building a security proxy hierarchy

You build security proxy hierarchies by adding an OVP to the security proxy class. You can use this property to create parent-child relationships between security proxies. Permissions are inherited all the way down the line of security proxies, and then to the case folders.



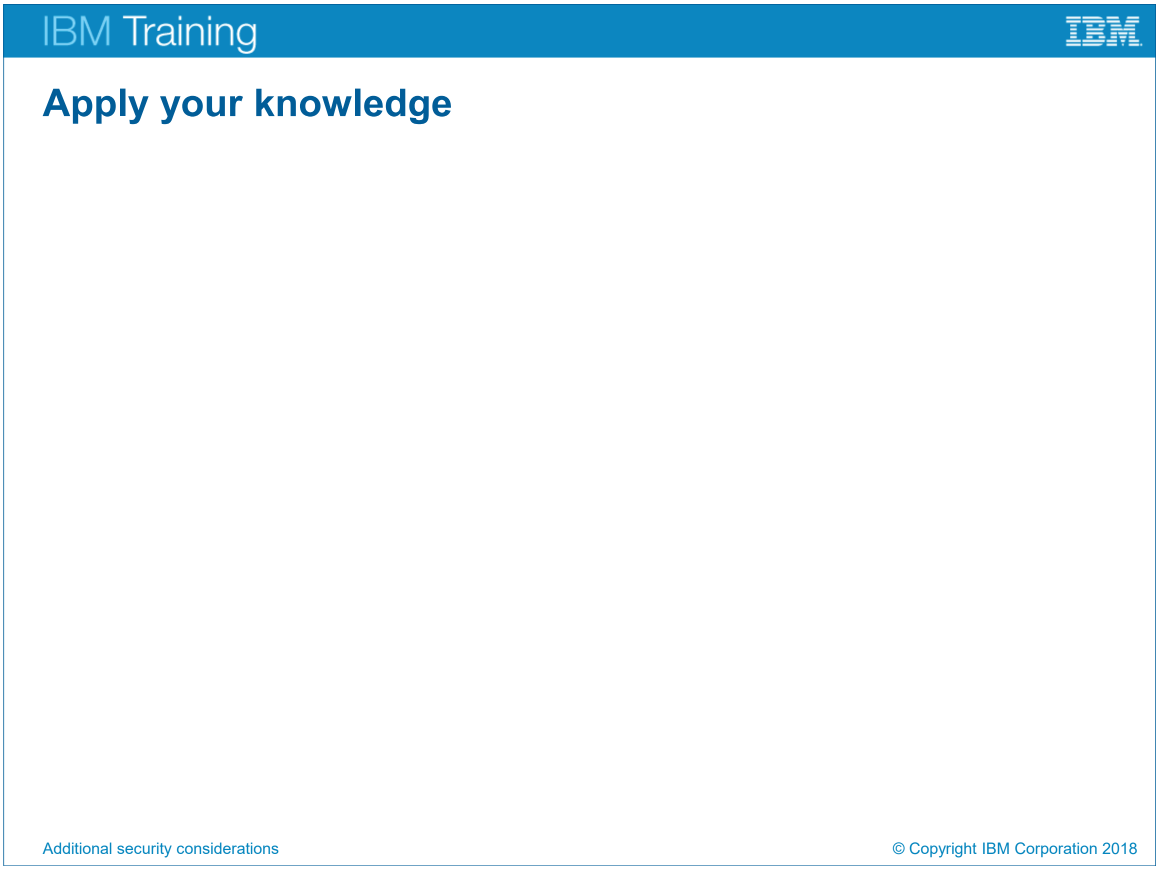
IBM Training

Unit summary

- Analyze scenarios that require specific security customizations

Additional security considerations

Unit summary



IBM Training

Apply your knowledge

Additional security considerations

Apply your knowledge

Apply your knowledge

In this unit you learned about a few specific security scenarios that require special considerations. Demonstrate mastery of this knowledge by correctly answering the quiz questions.

For each question, indicate the correct answer or best answer.

Questions

1. How is document security handled by IBM Case Manager by default?

   a. Inheritance

   b. Security proxy

   c. User-specified

   d. Default instance

2. Why use filter expressions to configure event subscriptions for changing an OVP value?

   a. To ensure that the event occurs only when the case state changes to a specific value

   b. To reduce the number of events launching workflows simultaneously

   c. To obtain the security proxy symbolic name to use in the CE_Operations component queue

   d. Filter expression is a required attribute for an event subscription

3. Why create a security proxy hierarchy?

   a. To dynamically change security on cases as the cases change state

   b. To reuse case types between business units without sharing case data

   c. To avoid having to rely on the Security Configuration to handle case security

   d. To ensure that case workers and solution architects can dynamically access documents filed in case folders

Answers

1. How is document security handled by IBM Case Manager by default?

   d. Default instance – Correct Answer

2. Why use filter expressions to configure event subscriptions for changing an OVP value?

   a. To ensure that the event occurs only when the case state changes to a specific value – Correct Answer

3. Why create a security proxy hierarchy?

   b. To reuse case types between business units without sharing case data – Correct Answer

IBM Training