Course Guide

IBM Case Foundation 5.2.1: Security

Course code F232 ERC 2.0

IBM Training

September 2016 edition

Notices

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

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

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 jurisdictions 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 provide 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 actual people or business enterprises is entirely coincidental.

Trademarks

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

Contents

Trademarks

The reader should recognize that the following terms, which appear in the content of this training document, are official trademarks of IBM or other companies:

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide.

The following are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide:

DB2®
FileNet®
Tivoli®
WebSphere®

Lenovo and ThinkPad are trademarks or registered trademarks of Lenovo in the United States, other countries, or both.

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

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

VMware and the VMware "boxes" logo and design, Virtual SMP and VMotion are registered trademarks or trademarks (the "Marks") of VMware, Inc. in the United States and/or other jurisdictions.

Other product and service names might be trademarks of IBM or other companies.

Course description

IBM Case Foundation 5.2.1: Security

Duration: 2 hours

Purpose

This course is designed to introduce workflow system security concepts, and to provide practice working with workflow system security. You work with an IBM Case Foundation 5.2.1 system to complete lesson exercises.

Audience

A Workflow System Administrator is responsible for day-to-day operations of a production IBM Case Foundation workflow application.

A Workflow System Administrator is typically required to help workflow participants to do the following tasks:

- Locate work and complete workflows.
- Respond to management decisions that require changes to work items.
- Gather information about workflow activity to help management make business decisions.

A Workflow Author is responsible for planning, designing, developing, and testing a workflow application within a development environment.

Prerequisites

Prerequisite skills and knowledge for this unit are:

- Familiarity with Windows 2008 operating systems.
- General knowledge of P8 Platform security concepts.
- General workflow terminology:
  - Workflow
  - Workflow definitions
  - Queues
  - Rosters.
- Start a P8 Platform system.
- Familiarity with P8 Platform administration interfaces, including:
  - Administration Console for Content Platform Engine
  - IBM Content Navigator
  - Process Configuration Console
  - Process Designer

Objectives

After completing this course, you should be able to:

- Inspect workflow system security settings.
- Identify and resolve workflow system security-related issues.
- Configure security for a workflow system.

Contents

Curriculum relationship

This section covers the courses planned for IBM Case Foundation 5.2.1. Refer to the IBM Training Paths for the curriculum relationship. The training paths will be updated as courses become available.

IBM Training Paths

http://www-304.ibm.com/jct03001c/services/learning/ites.wss/us/en?pageType=page&c=Y678448H04759K32

The courses are available as single SPVC modules, or multi-day courses delivered as instructor-lead training. Here is a list of the modules organized by roles. Some of the modules apply to multiple roles.

Solution Architect

- Introduction
- Workflow security

Workflow system administrator:

- Introduction
- Configure the workflow system
- Workflow security
- Maintain the workflow system
- Manage Work in Progress
- Migrate and deploy workflow applications
- Component Integration
- Workflow Analysis tools

Unit 1. IBM Case Foundation 5.2.1: Security

Estimated time

00:00

Overview

You learn how to configure and administer security for an IBM Case Foundation workflow system.

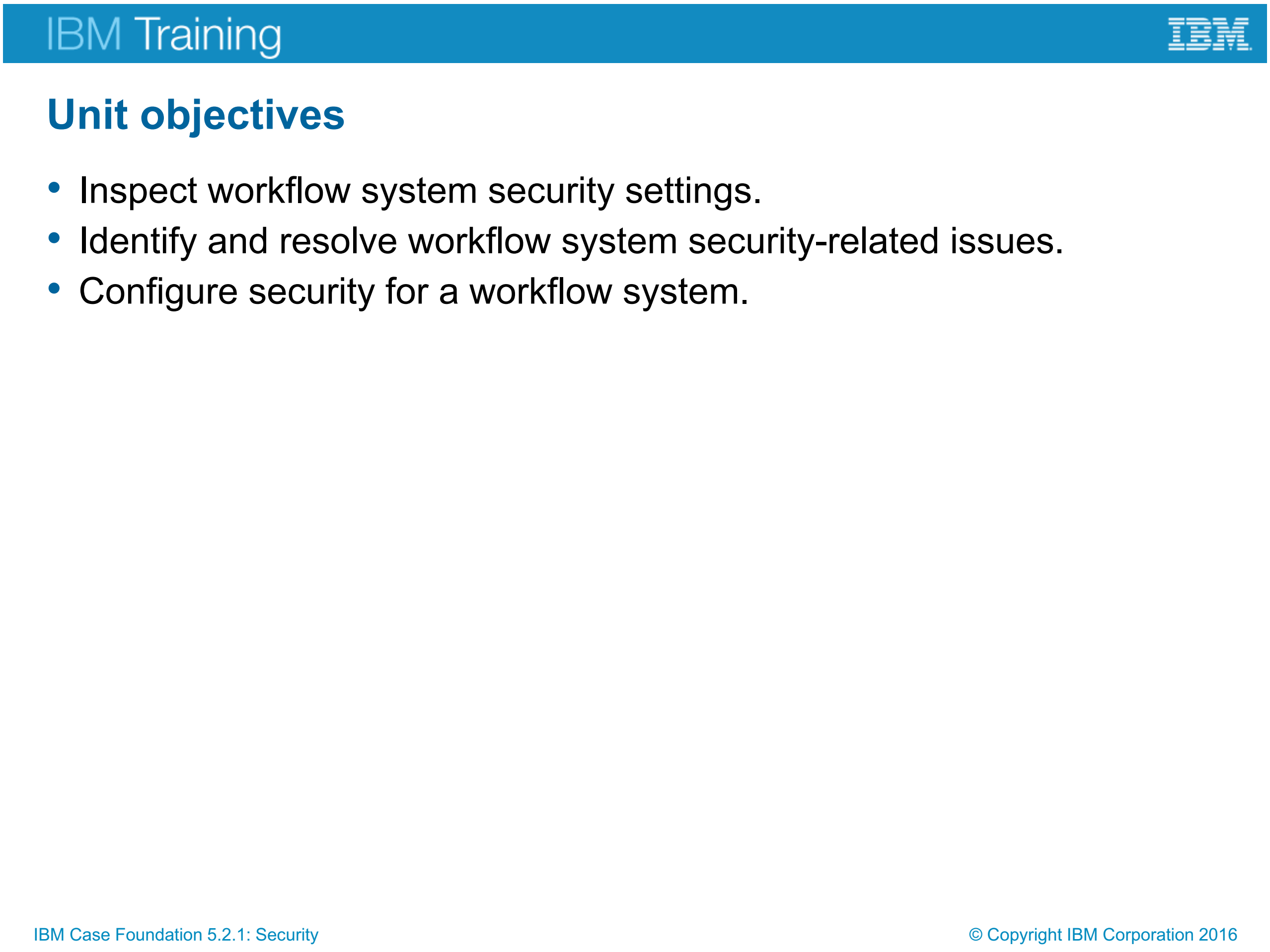
How you will check your progress

- Successfully complete the lesson exercises.

References

IBM Knowledge Connection URL:

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8toc.doc/welcome_p8.htm



IBM Training

Unit objectives

- Inspect workflow system security settings.
- Identify and resolve workflow system security-related issues.
- Configure security for a workflow system.

IBM Case Foundation 5.2.1: Security

Figure 1-1. Unit objectives

Lesson 1.1. Security overview

IBM Training

Security overview

IBM Case Foundation 5.2.1: Security

© Copyright IBM Corporation 2016

Figure 1-2. Security overview

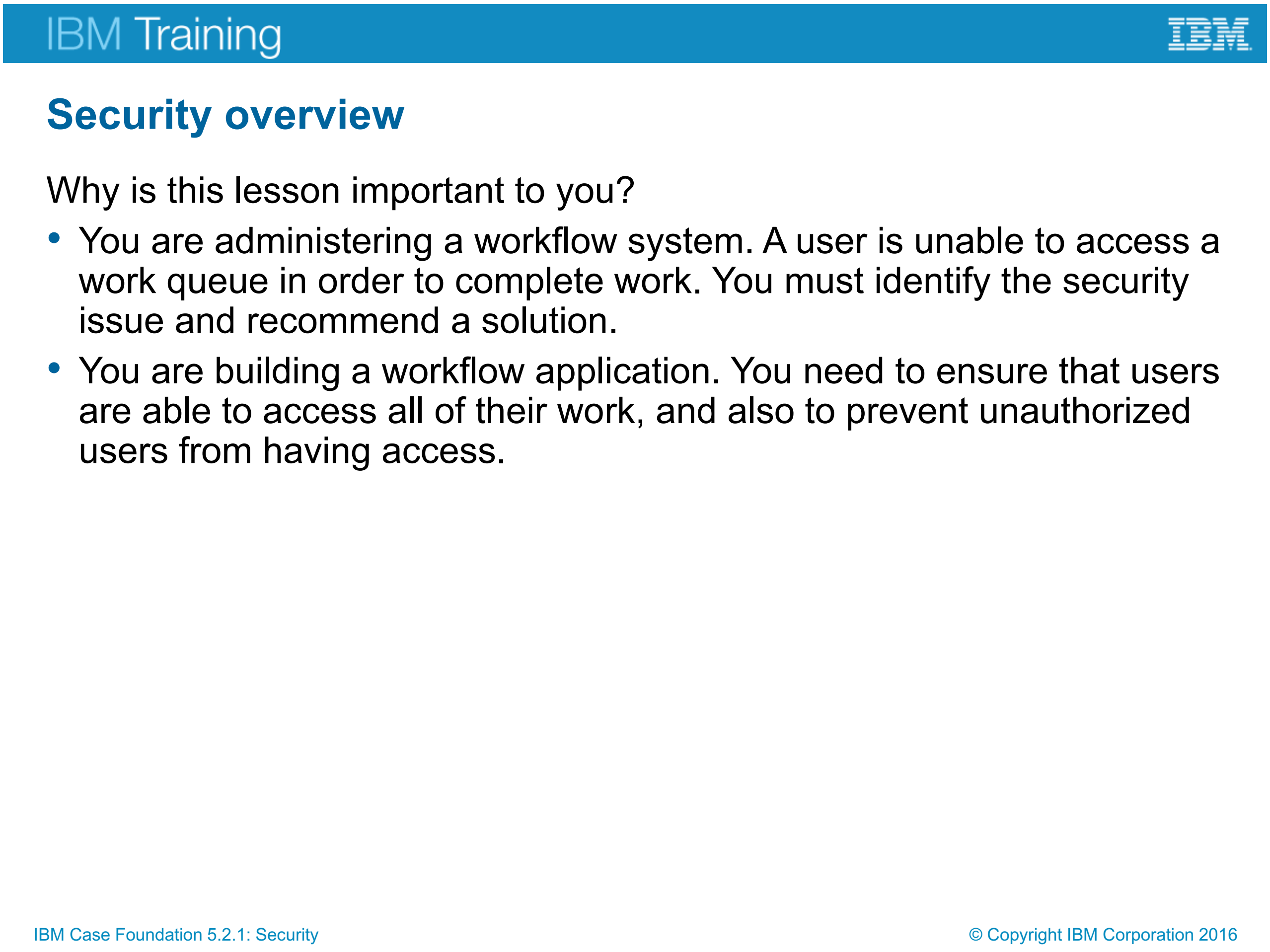
IBM Training

Lessons

▶ Security overview
- Security configuration

IBM Case Foundation 5.2.1: Security

Figure 1-3. Lessons



IBM Training

Security overview

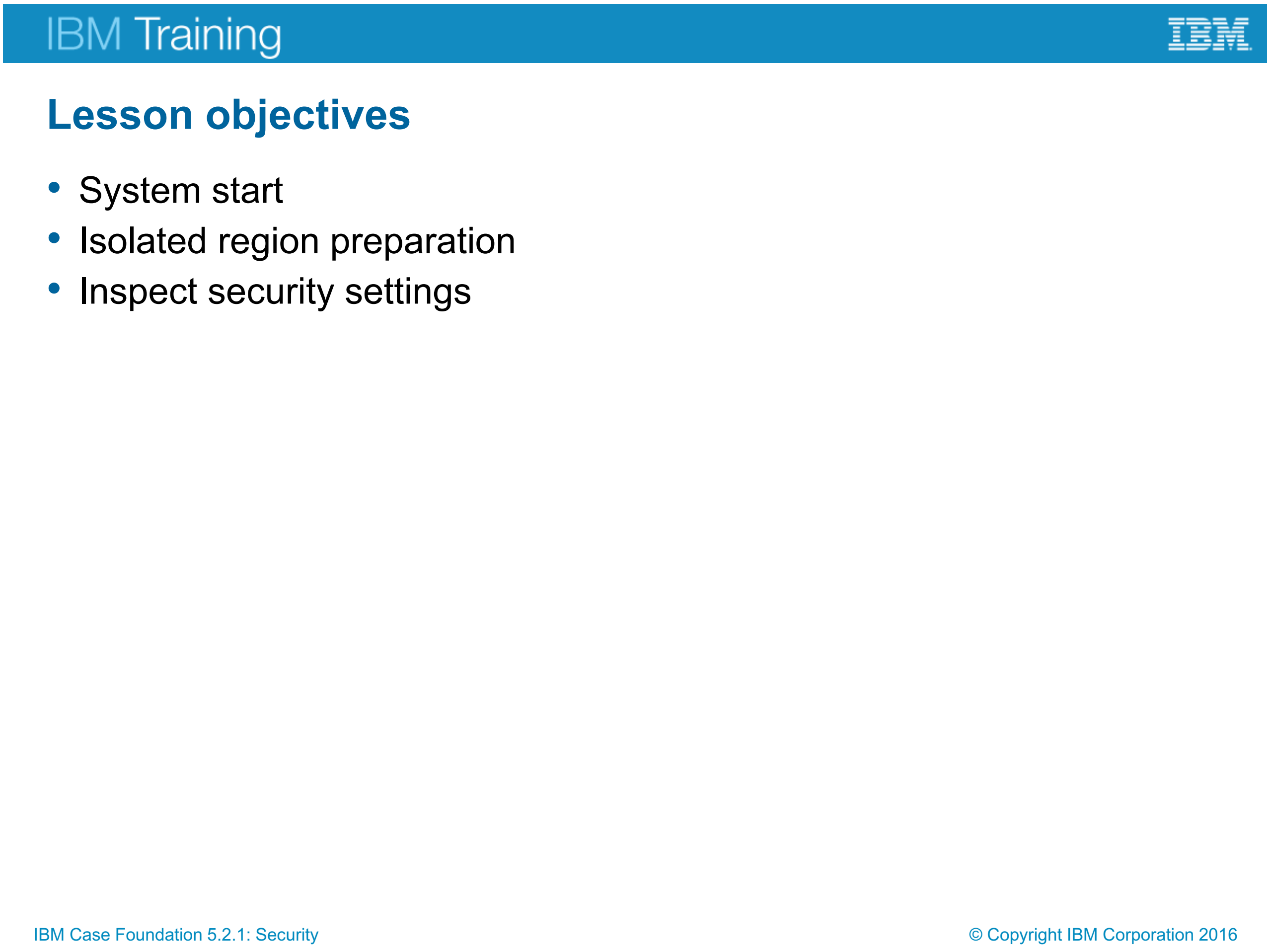
Why is this lesson important to you?

- You are administering a workflow system. A user is unable to access a work queue in order to complete work. You must identify the security issue and recommend a solution.
- You are building a workflow application. You need to ensure that users are able to access all of their work, and also to prevent unauthorized users from having access.

IBM Case Foundation 5.2.1: Security

© Copyright IBM Corporation 2016

Figure 1-4. Security overview



IBM Training

Lesson objectives

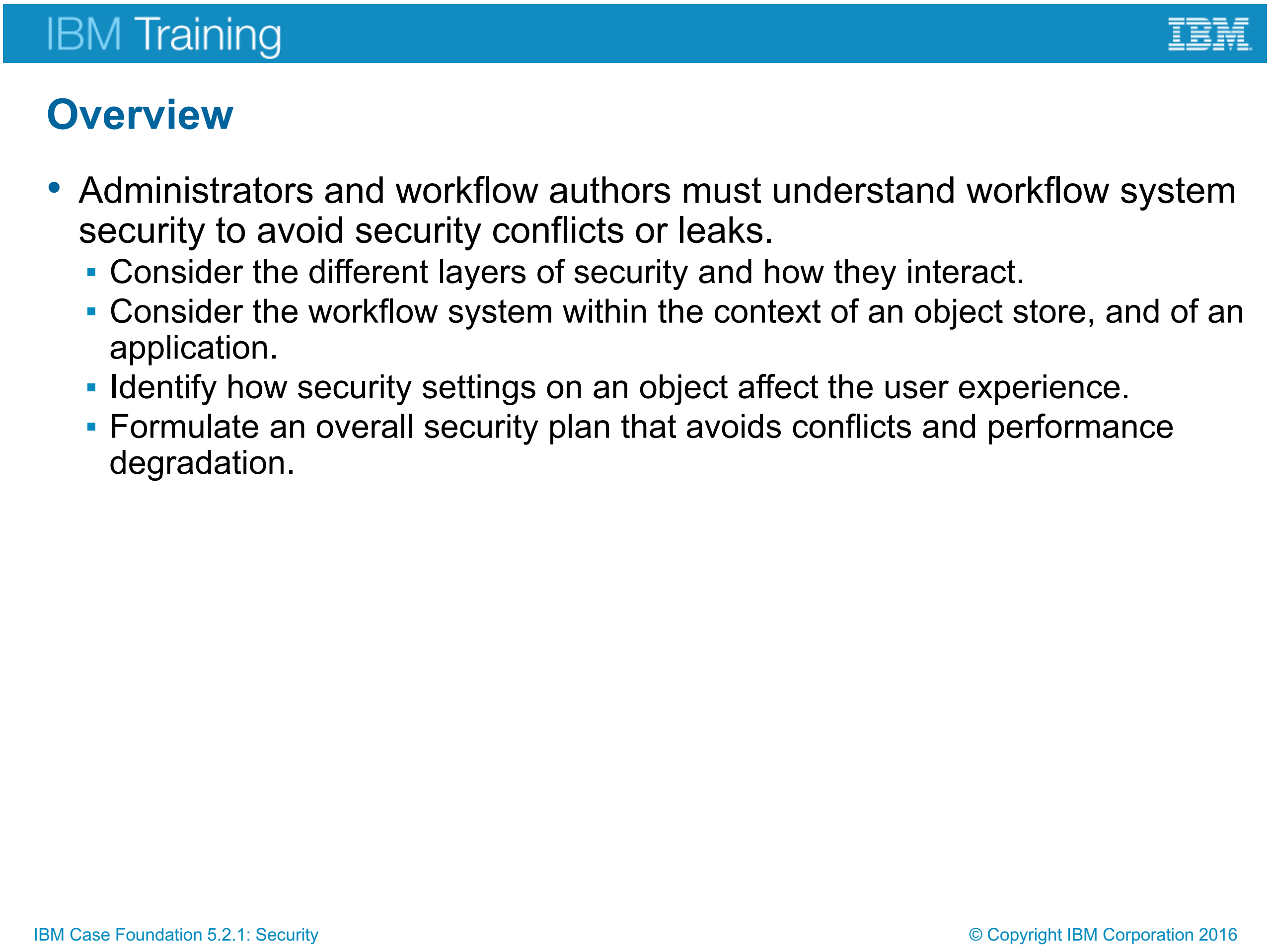
- System start
- Isolated region preparation
- Inspect security settings

IBM Case Foundation 5.2.1: Security

© Copyright IBM Corporation 2016

Figure 1-5. Lesson objectives

You need to complete these activities in this lesson.



IBM Training

Overview

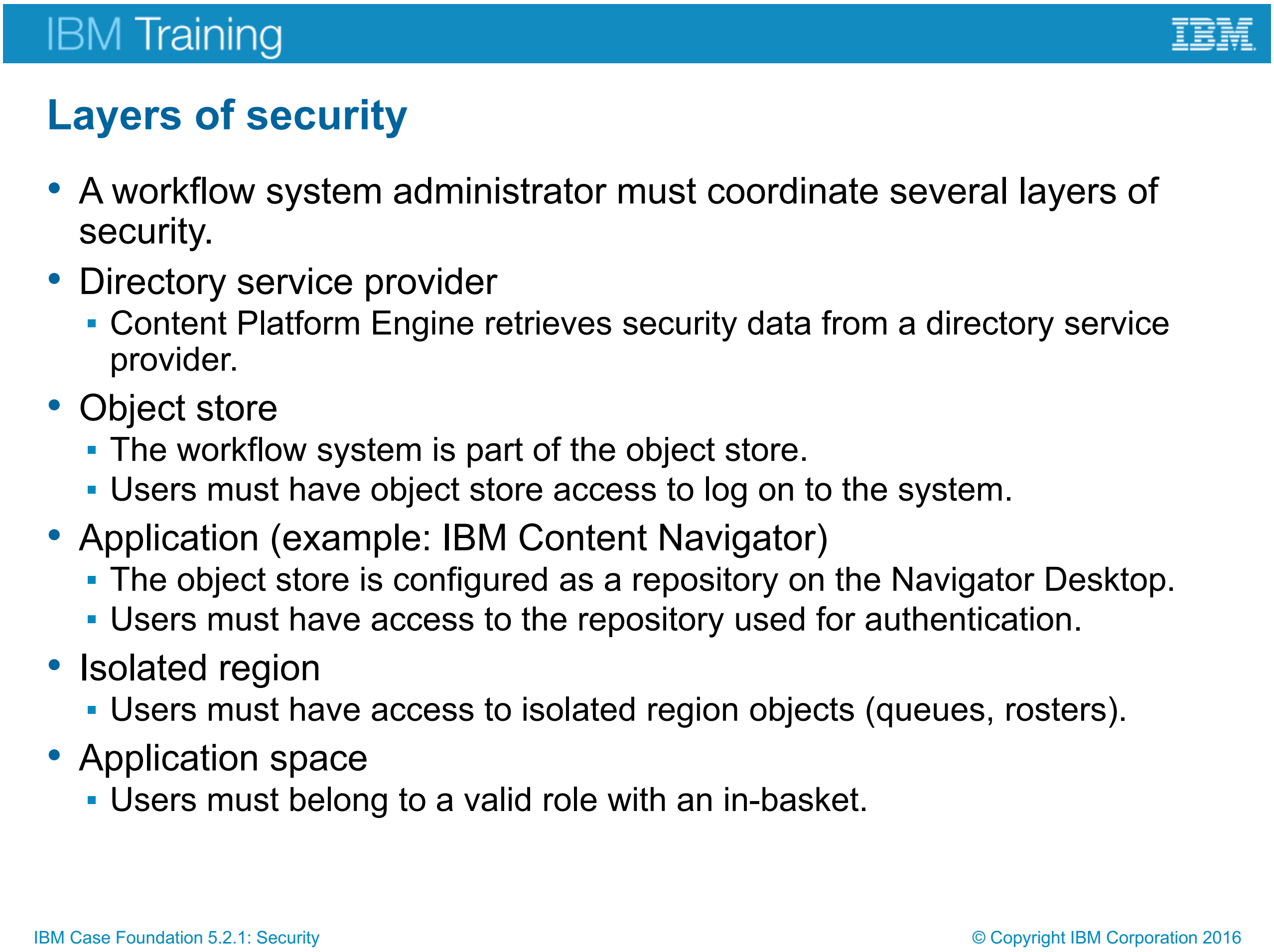
- Administrators and workflow authors must understand workflow system security to avoid security conflicts or leaks.
  - Consider the different layers of security and how they interact.
  - Consider the workflow system within the context of an object store, and of an application.
  - Identify how security settings on an object affect the user experience.
  - Formulate an overall security plan that avoids conflicts and performance degradation.

IBM Case Foundation 5.2.1: Security

© Copyright IBM Corporation 2016

Figure 1-6. Overview

Help path



IBM Training

Layers of security

- A workflow system administrator must coordinate several layers of security.
- Directory service provider
  - Content Platform Engine retrieves security data from a directory service provider.
- Object store
  - The workflow system is part of the object store.
  - Users must have object store access to log on to the system.
- Application (example: IBM Content Navigator)
  - The object store is configured as a repository on the Navigator Desktop.
  - Users must have access to the repository used for authentication.
- Isolated region
  - Users must have access to isolated region objects (queues, rosters).
- Application space
  - Users must belong to a valid role with an in-basket.

IBM Case Foundation 5.2.1: Security

© Copyright IBM Corporation 2016

Figure 1-7. Layers of security

Help paths

- FileNet P8 Platform 5.2.1>Security>Directory service providers
  - http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psd000.htm
- FileNet P8 Platform 5.2.1>Administering>Administering Content Platform Engine>Defining the FileNet P8 infrastructure>FileNet P8 domains
  - http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.ce.admin.tasks.doc/aboutem/dom_concepts.htm
- FileNet P8 Platform 5.2.1>Security>Authentication>JAVA-based client authentication (JAAS)>Browser-based clients of Java EE application servers
  - http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psn007.htm

Directory service provider

Content Platform Engine server does not implement its own authentication module. Instead, it uses a Java Platform Enterprise Edition (Java EE) application server's authentication mechanism. The FileNet P8 domain provides the security context for authenticating applications. A FileNet P8 domain is associated with one or more Java EE security policy domains. The Java EE domain is used to authenticate users and establish their group memberships. Identity and group membership of the user determine which FileNet P8 domain objects the user can access.

Object Store

Each object store has its own access control list (ACL). Each object store can have a different set of administrators. The object store creator adds Administrator and user groups to the object store when the object store is created. By default, administrative users have Full Control, and non-administrative groups have Use Object Store access, which gives certain read and write privileges. Object store security uses an inheritance model, starting from the object store, and working down through object classes. Security can be further configured on object classes, containers, and objects themselves.

Application

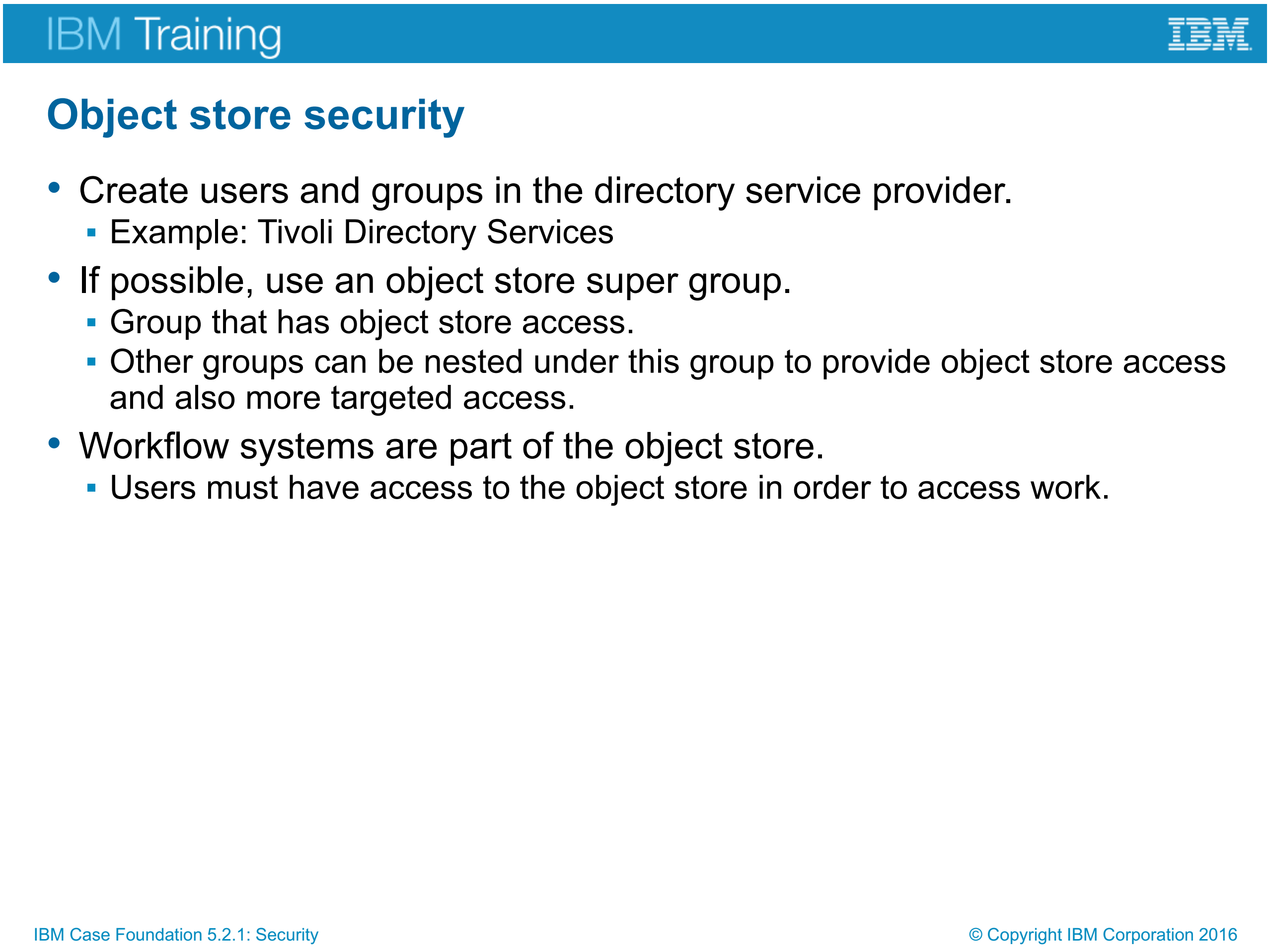
Browser-based clients of Java EE-based application servers interact with servlets and JavaServer Pages (JSPs). The two types of browser-based application security exist: Application-managed authentication, and Container-managed authentication. The type authentication is configured during the application installation.

Isolated region

Isolated region objects: queues, rosters, event logs, are independently secured.

Application Space

You define roles in the application space. Roles control access to in-baskets that are associated with user and work queues.



IBM Training

Object store security

- Create users and groups in the directory service provider.
  - Example: Tivoli Directory Services
- If possible, use an object store super group.
  - Group that has object store access.
  - Other groups can be nested under this group to provide object store access and also more targeted access.
- Workflow systems are part of the object store.
  - Users must have access to the object store in order to access work.

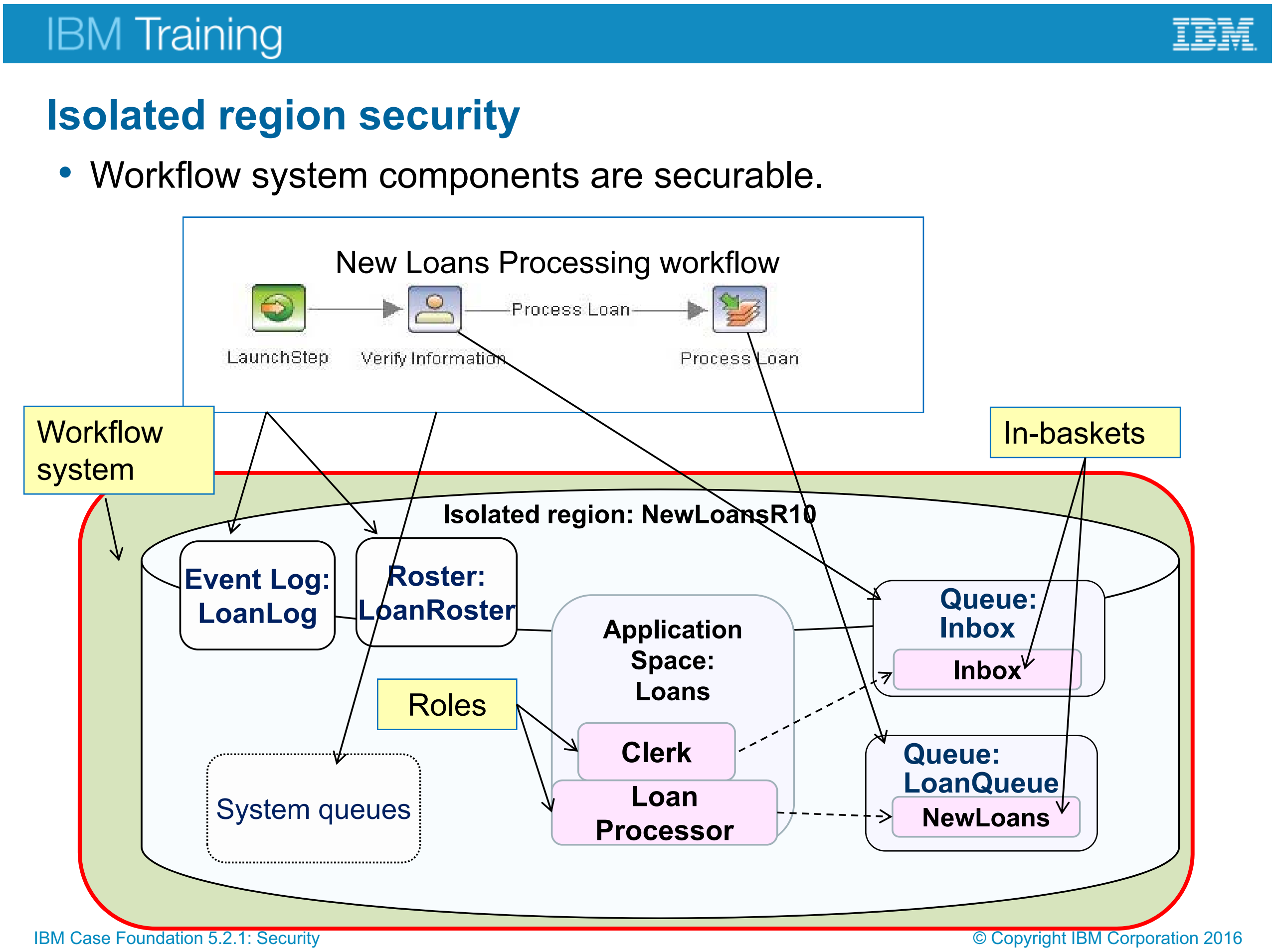
IBM Case Foundation 5.2.1: Security

© Copyright IBM Corporation 2016

Figure 1-8. Object store security

Help path

A super group is an LDAP 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 super group.



IBM Training

Isolated region security

- Workflow system components are securable.

IBM Case Foundation 5.2.1: Security

© Copyright IBM Corporation 2016

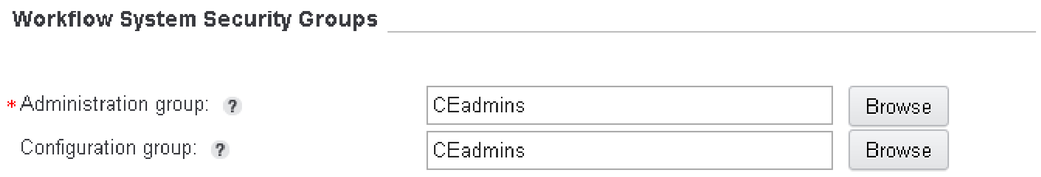
Figure 1-9. Isolated region security

The workflow system contains objects that are independently secured. Problems can arise when security is not planned carefully to avoid possible conflicts.

IBM Training

Workflow system security groups

- A workflow system has two special security groups:
  - Administration group can open Process Administrator.
  - Configuration group can open Process Configuration Console and access isolated region objects in Administration Console.
- The security groups are defined on the Workflow System page in Administration Console.
  - Only one entry is allowed for each group.



Workflow System Security Groups

*Administration group: ? CEadmins

Configuration group: ? CEadmins

IBM Case Foundation 5.2.1: Security

Figure 1-10. Workflow system security groups

Help paths

FileNet P8 Platform 5.2.1>Security>Users and groups required by FileNet P8>Directory server accounts>Workflow system administrator

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psu054.htm

FileNet P8 Platform 5.2.1>Security>Users and groups required by FileNet P8>Directory server accounts>Workflow system administrator group

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psu027.htm

FileNet P8 Platform 5.2.1>Security>Users and groups required by FileNet P8>Directory server accounts>Workflow system configuration group

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psu028.htm

Usually, the Administration Group and the Configuration Group are separate groups.

Administration Group

The Administration Group is a required field when the workflow system is created. The user who is creating the workflow system must be in the Administration Group. Administrator groups can run the configuration tools by default. . Only groups that have administration privileges on the FileNet P8 Domain can be added to the Administration Group.

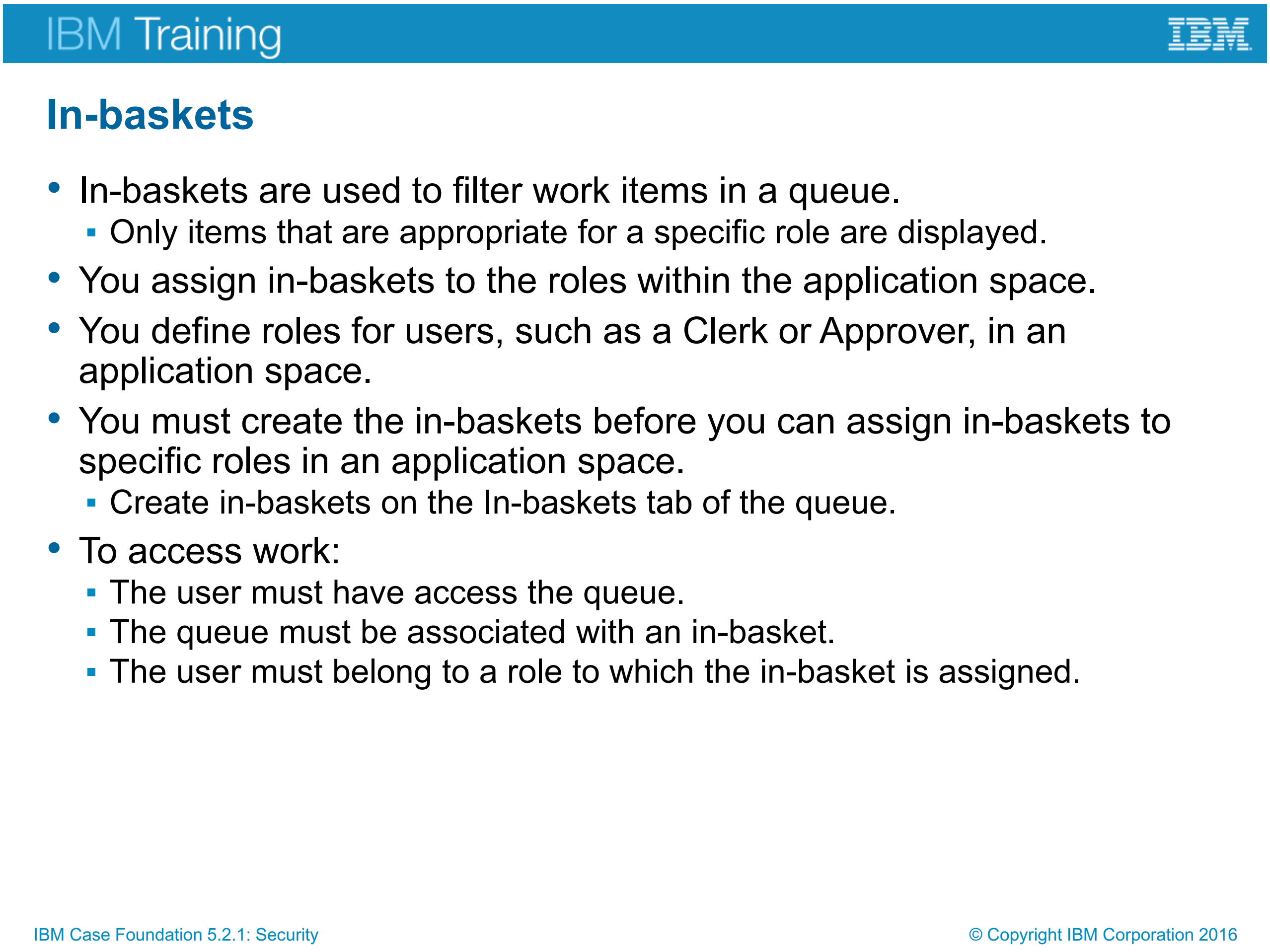
Configuration Group

The Configuration Group allows users to open the Process Configuration Console and Process Designer. If you are in the Configuration Group, you can access the isolated region objects from Administration Console.

The Configuration Group field can be left blank. If you leave the Configuration Group field blank, anyone with access to the object store can create queues, rosters, change security on queues rosters, and even delete the connection point and isolated region. Do not leave this field blank on a production system.

Changing groups

In most scenarios, these groups are added at the beginning of the implementation and remain. Individual users can be added to either group on the directory server. In those rare instances in which you do want to change the Administration Group, you must be a member of the target group, and you must restart the application for the changes to take effect.



IBM Training

In-baskets

- In-baskets are used to filter work items in a queue.
  - Only items that are appropriate for a specific role are displayed.
- You assign in-baskets to the roles within the application space.
- You define roles for users, such as a Clerk or Approver, in an application space.
- You must create the in-baskets before you can assign in-baskets to specific roles in an application space.
  - Create in-baskets on the In-baskets tab of the queue.
- To access work:
  - The user must have access the queue.
  - The queue must be associated with an in-basket.
  - The user must belong to a role to which the in-basket is assigned.

IBM Case Foundation 5.2.1: Security

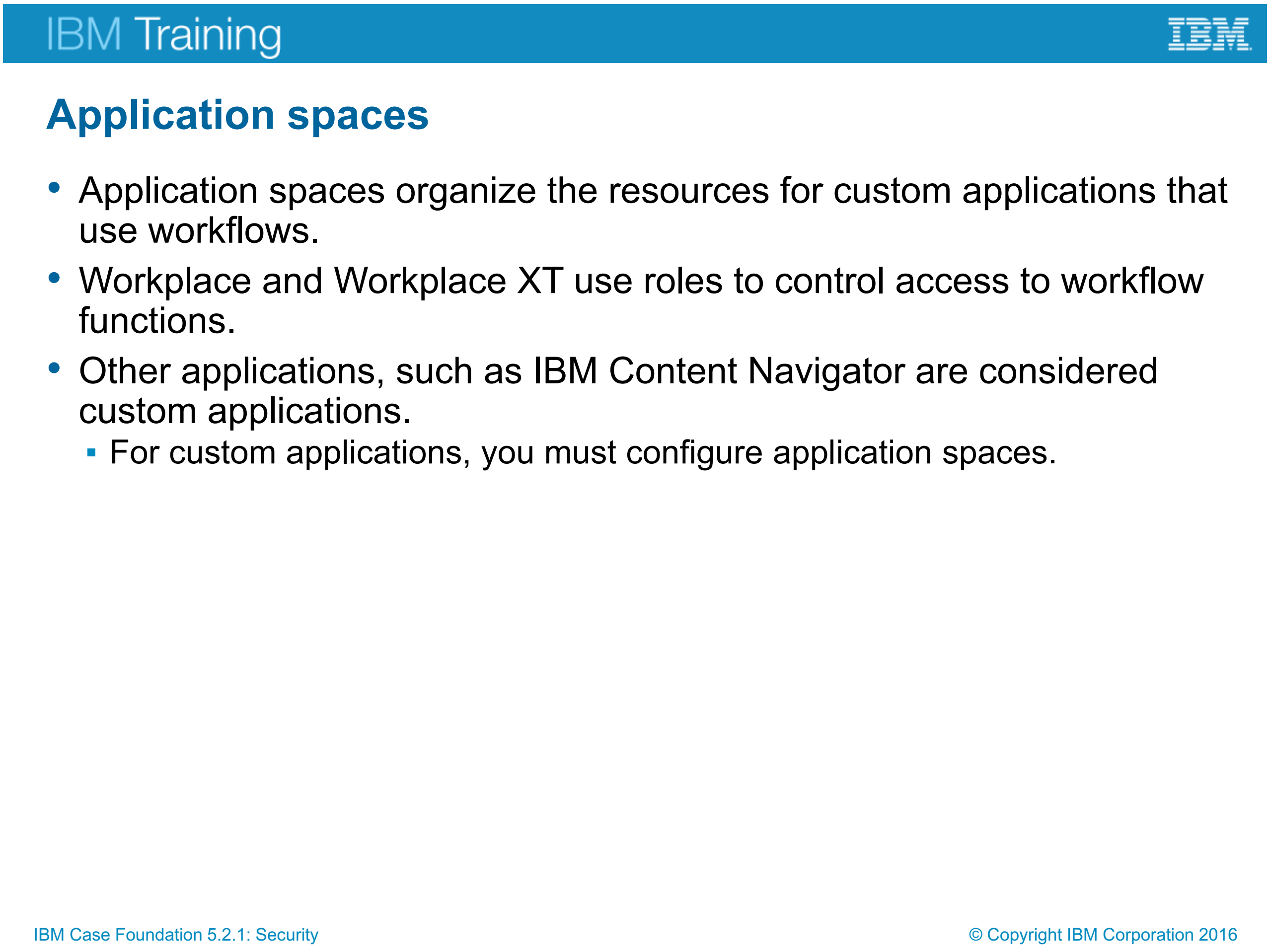
© Copyright IBM Corporation 2016

Figure 1-11. In-baskets

Help path

FileNet P8 Platform 5.2.1>Administering>Administering Content Platform Engine>Defining the workflow system>Coordinating workflow design>Workflow options>In-baskets

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.ce.admin.tasks.doc/p8pcc316.htm



IBM Training

Application spaces

- Application spaces organize the resources for custom applications that use workflows.
- Workplace and Workplace XT use roles to control access to workflow functions.
- Other applications, such as IBM Content Navigator are considered custom applications.
  - For custom applications, you must configure application spaces.

IBM Case Foundation 5.2.1: Security

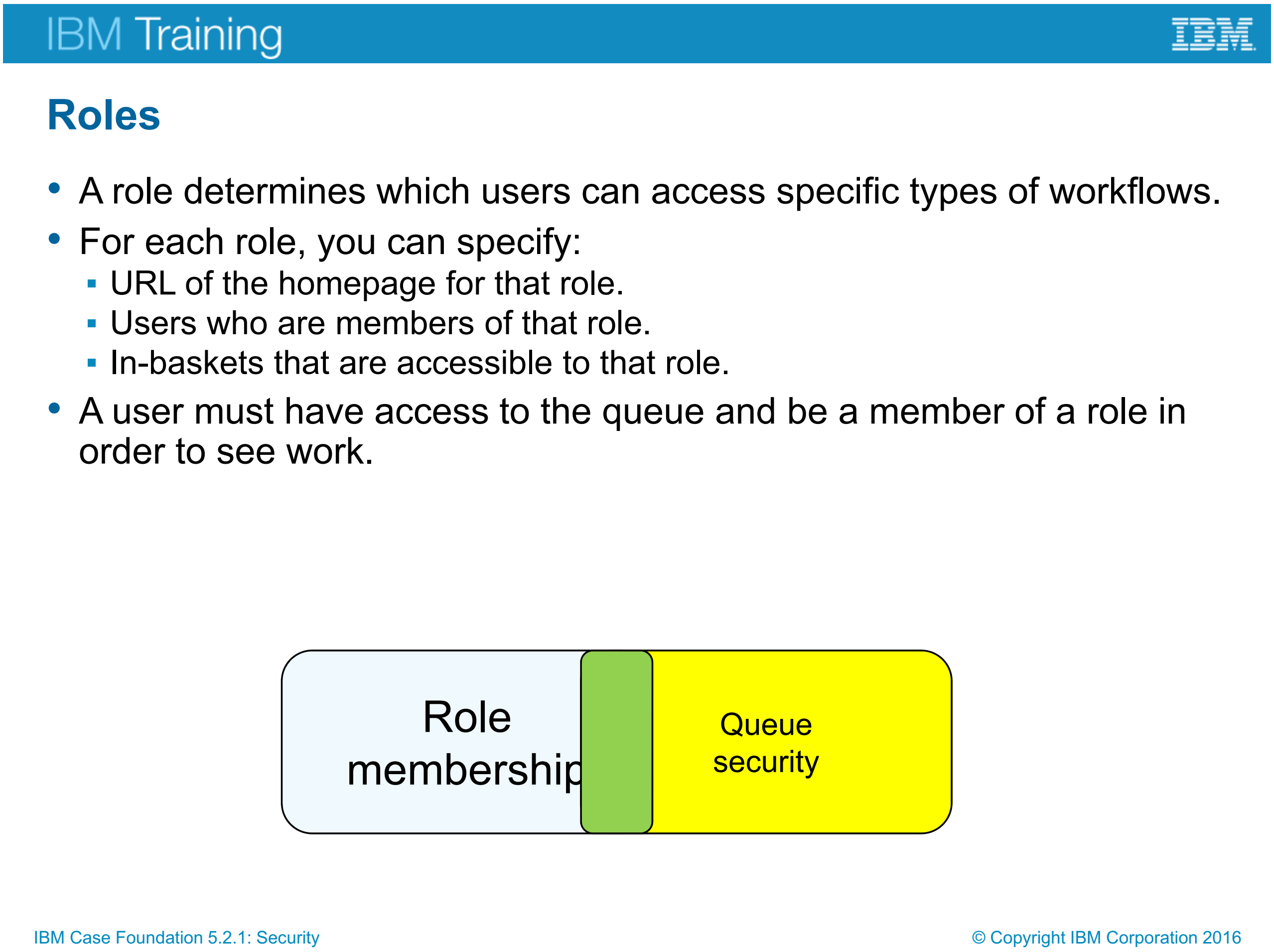
© Copyright IBM Corporation 2016

Figure 1-12. Application spaces

Help path

FileNet P8 Platform 5.2.1>Administering>Administering Content Platform Engine>Defining the workflow system>Coordinating workflow design>Workflow options>In-baskets>Creating application spaces

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.ce.admin.tasks.doc/p8pcc306.htm



IBM Training

Roles

- A role determines which users can access specific types of workflows.
- For each role, you can specify:
  - URL of the homepage for that role.
  - Users who are members of that role.
  - In-baskets that are accessible to that role.
- A user must have access to the queue and be a member of a role in order to see work.

Role membership
Queue security

IBM Case Foundation 5.2.1: Security

© Copyright IBM Corporation 2016

Figure 1-13. Roles

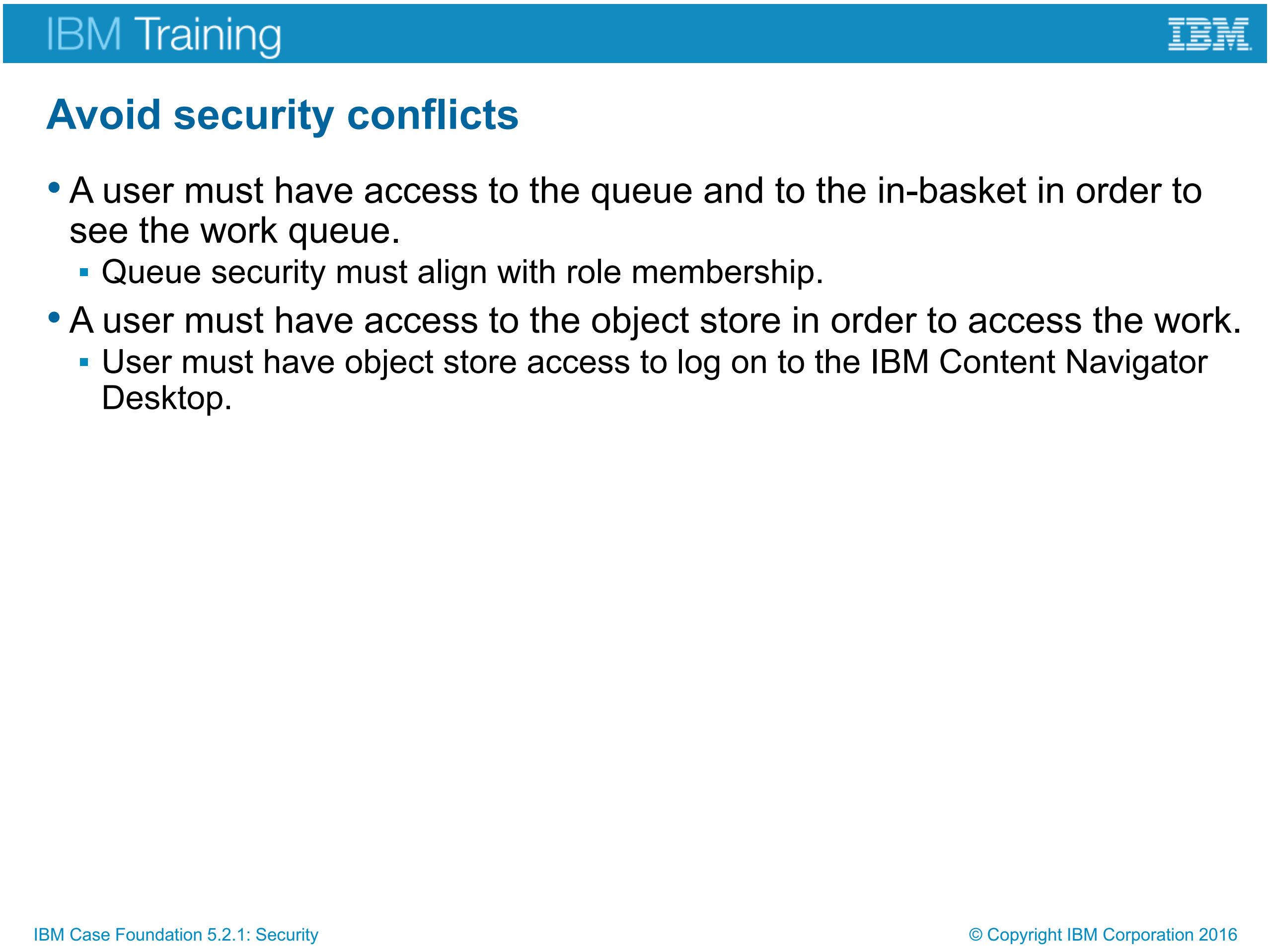
Help path

FileNet P8 Platform 5.2.0>Integrating workflow into document management>Configuring the workflow system>Manage application spaces>Creating roles

> http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.0/com.ibm.p8.pe.configui.doc/bpfc085.htm

You add roles to the application space. For each role, you must determine role members and which in-baskets are available to that role. If you leave the queues unsecured, anyone with access to the role would have access to the queues. Do not conclude that you can control security entirely by controlling role membership. A user can use custom API to access the queues, bypassing application security. Control security on the queues first, and then the roles to prevent unauthorized access to workflows.

If you add a user or group to a user or work queue, do not forget to edit the role membership. A user who has access to the queue cannot see the queue without being a member of the role that can access the associated in-basket.



IBM Training

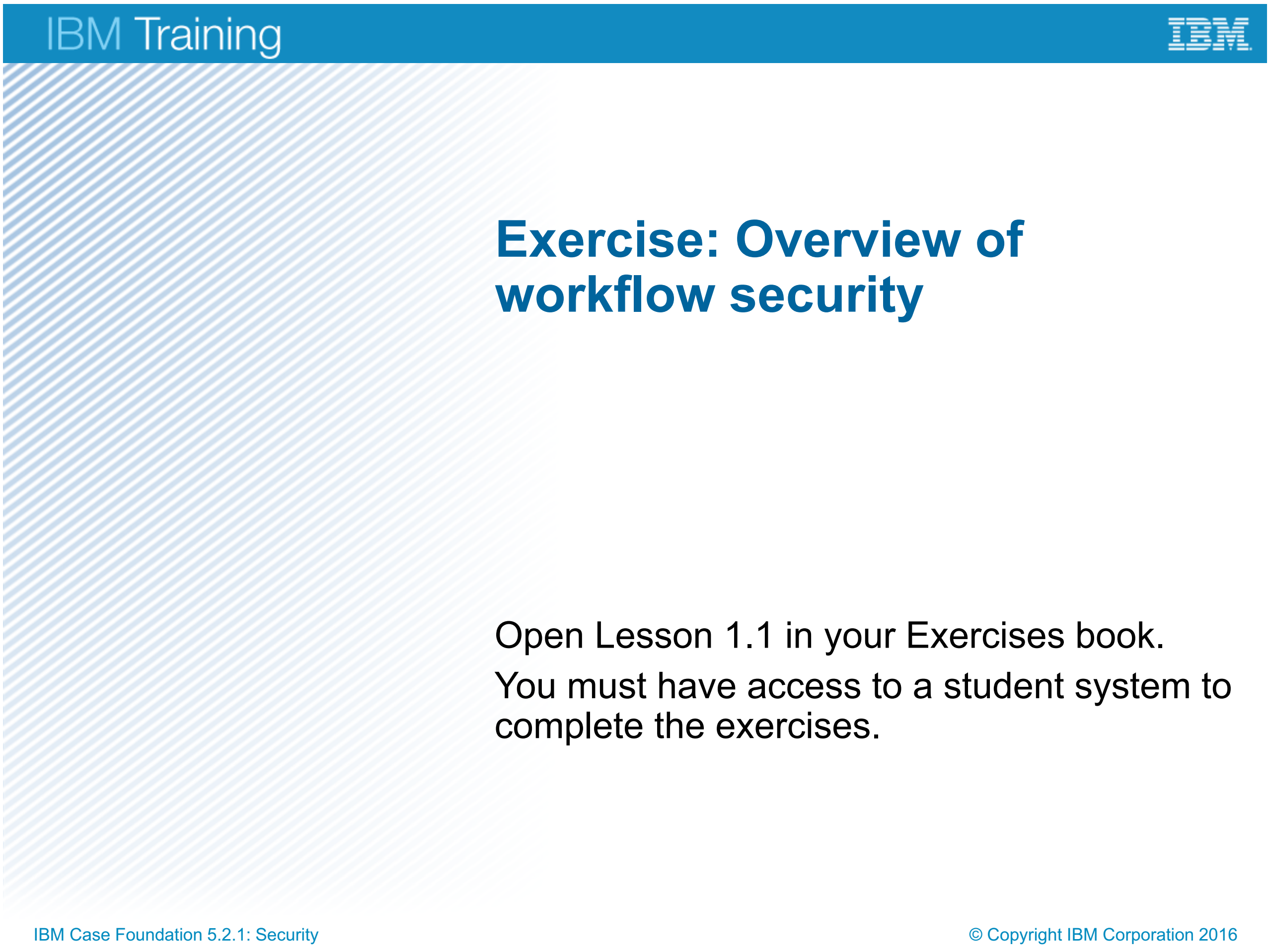
Avoid security conflicts

- A user must have access to the queue and to the in-basket in order to see the work queue.
  - Queue security must align with role membership.
- A user must have access to the object store in order to access the work.
  - User must have object store access to log on to the IBM Content Navigator Desktop.

IBM Case Foundation 5.2.1: Security

Figure 1-14. Avoid security conflicts

Help path



IBM Training

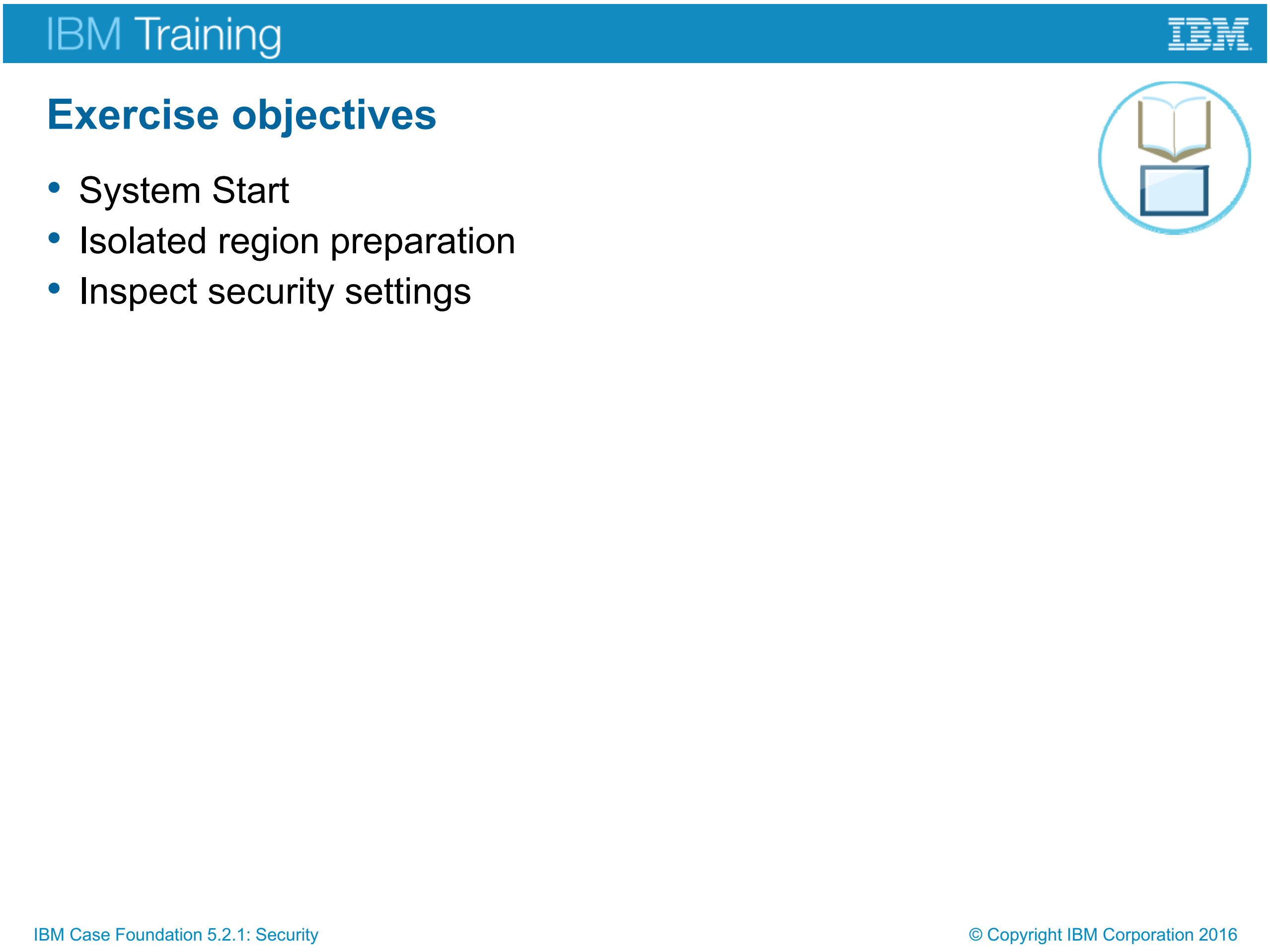
Exercise: Overview of workflow security

Open Lesson 1.1 in your Exercises book.

You must have access to a student system to complete the exercises.

IBM Case Foundation 5.2.1: Security

Figure 1-15. Exercise: Overview of workflow security



IBM Training

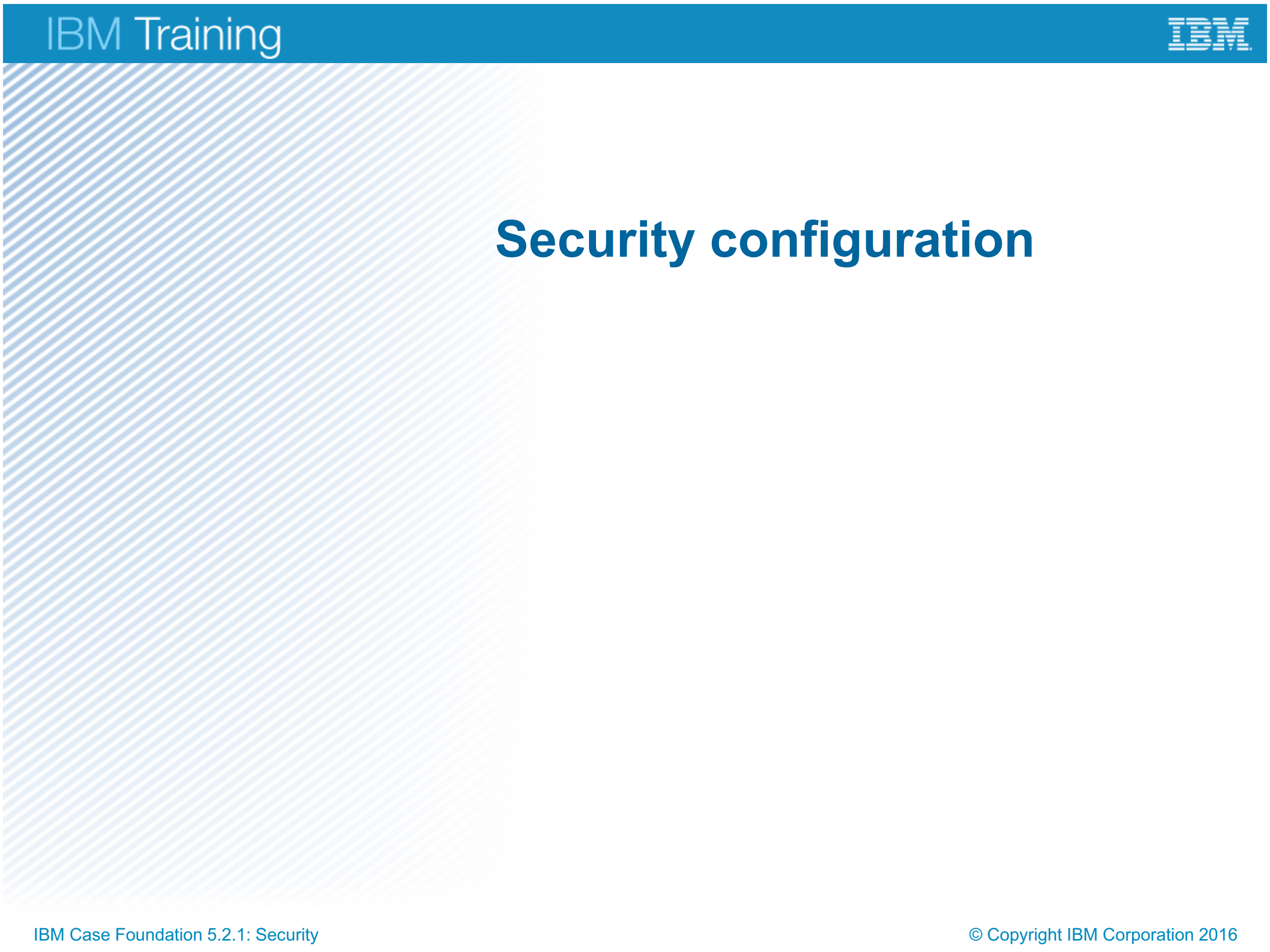
Exercise objectives

- System Start
- Isolated region preparation
- Inspect security settings

IBM Case Foundation 5.2.1: Security

Figure 1-16. Exercise objectives

Lesson 1.2. Security configuration



IBM Training

Security configuration

IBM Case Foundation 5.2.1: Security

Figure 1-17. Security configuration

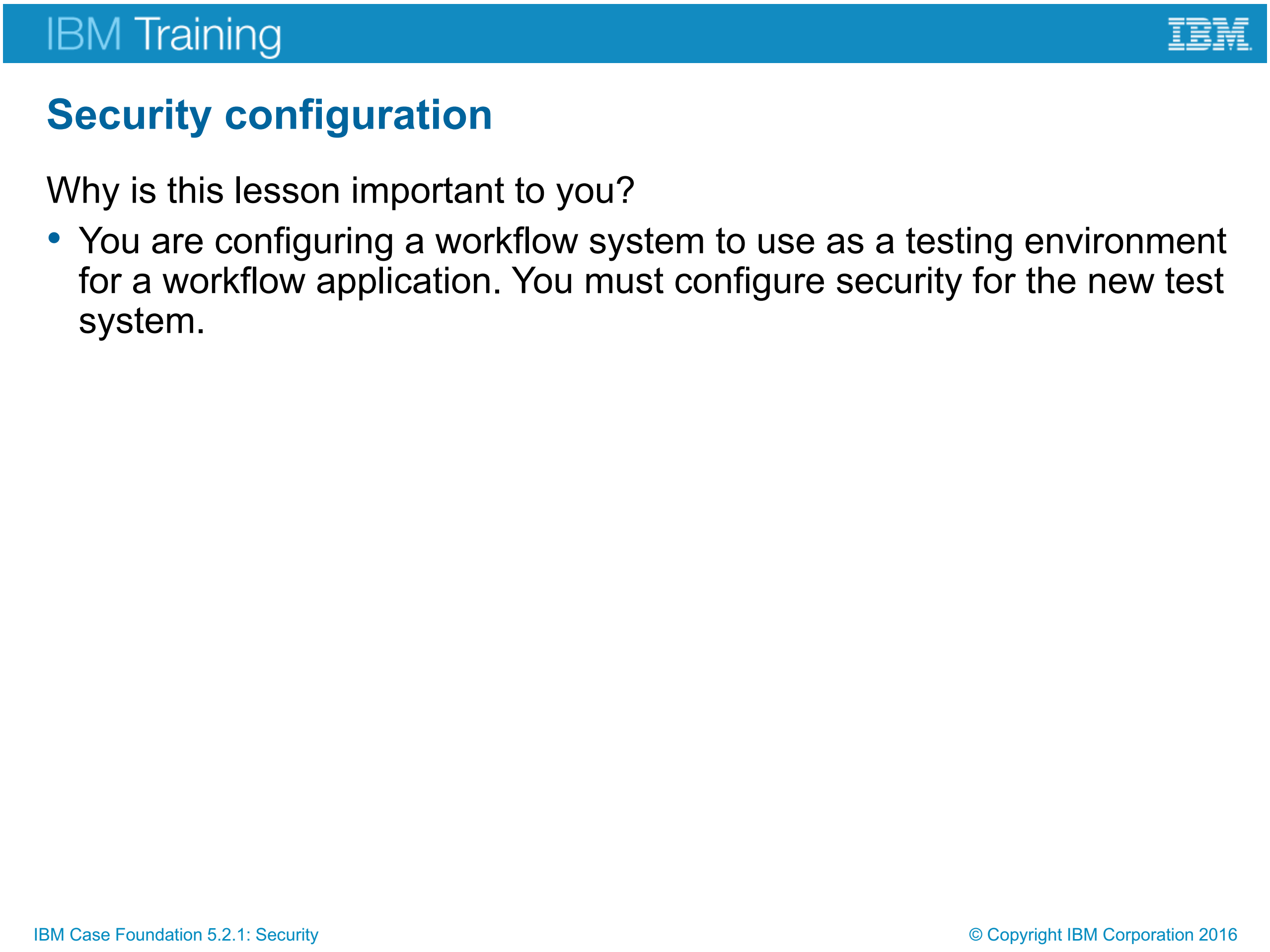
IBM Training IBM

Lessons

- Security overview
- ▶ Security configuration

IBM Case Foundation 5.2.1: Security © Copyright IBM Corporation 2016

Figure 1-18. Lessons



IBM Training

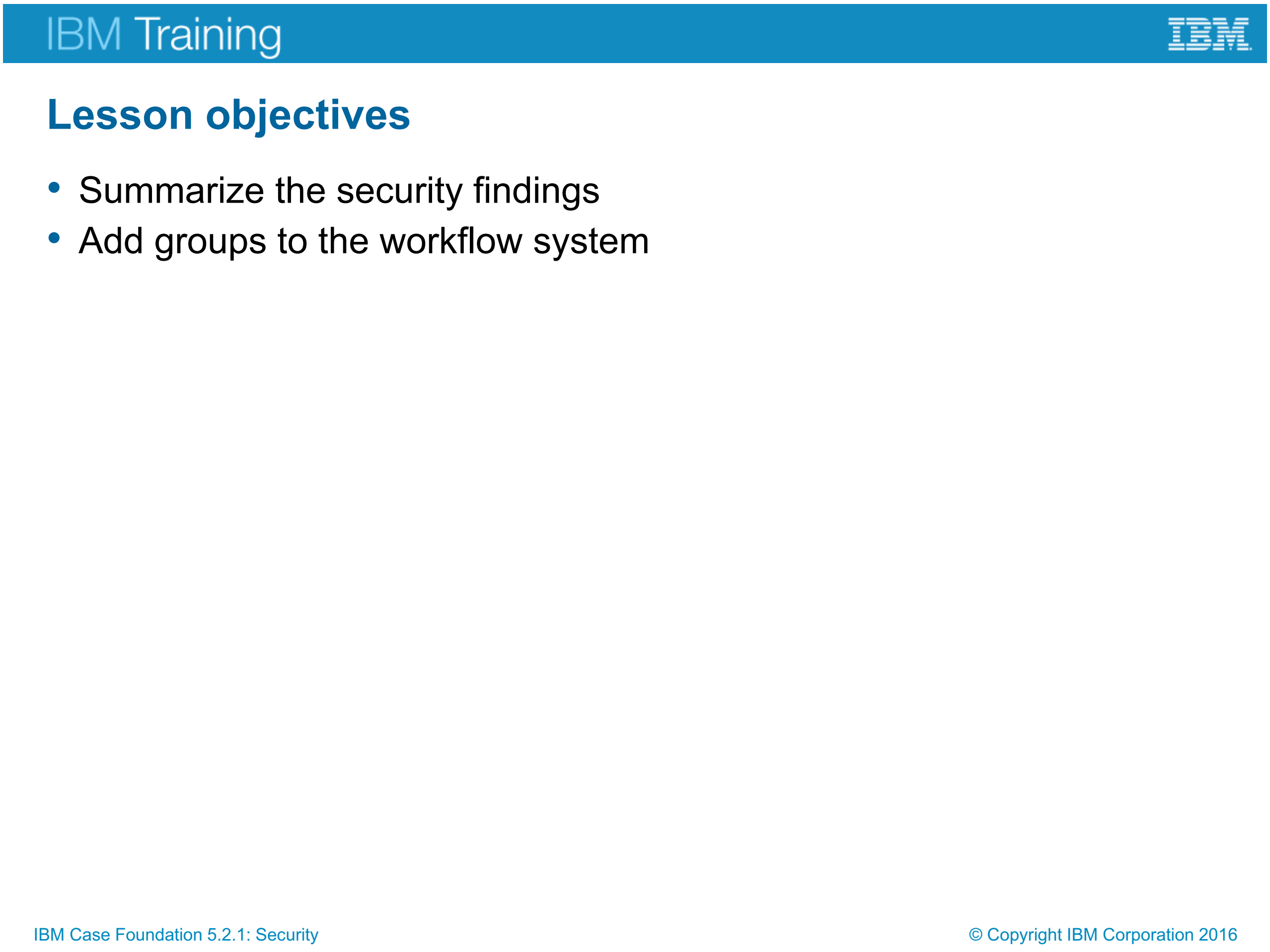
Security configuration

Why is this lesson important to you?

- You are configuring a workflow system to use as a testing environment for a workflow application. You must configure security for the new test system.

IBM Case Foundation 5.2.1: Security

Figure 1-19. Security configuration



IBM Training

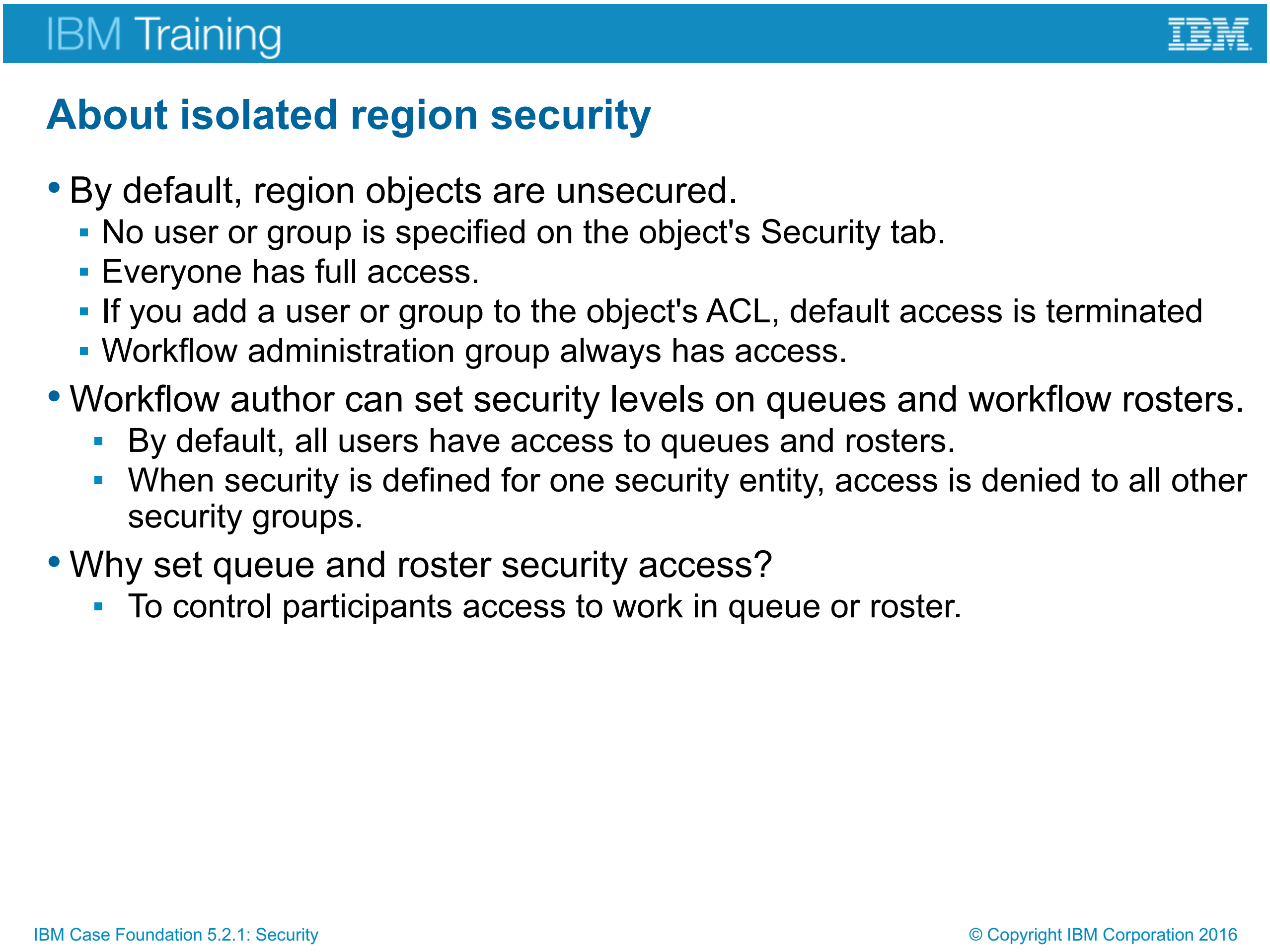
Lesson objectives

- Summarize the security findings
- Add groups to the workflow system

IBM Case Foundation 5.2.1: Security

Figure 1-20. Lesson objectives

You need to complete these activities in this lesson.



IBM Training

About isolated region security

- By default, region objects are unsecured.
  - No user or group is specified on the object's Security tab.
  - Everyone has full access.
  - If you add a user or group to the object's ACL, default access is terminated
  - Workflow administration group always has access.
- Workflow author can set security levels on queues and workflow rosters.
  - By default, all users have access to queues and rosters.
  - When security is defined for one security entity, access is denied to all other security groups.
- Why set queue and roster security access?
  - To control participants access to work in queue or roster.

IBM Case Foundation 5.2.1: Security

Figure 1-21. About isolated region security

Help path

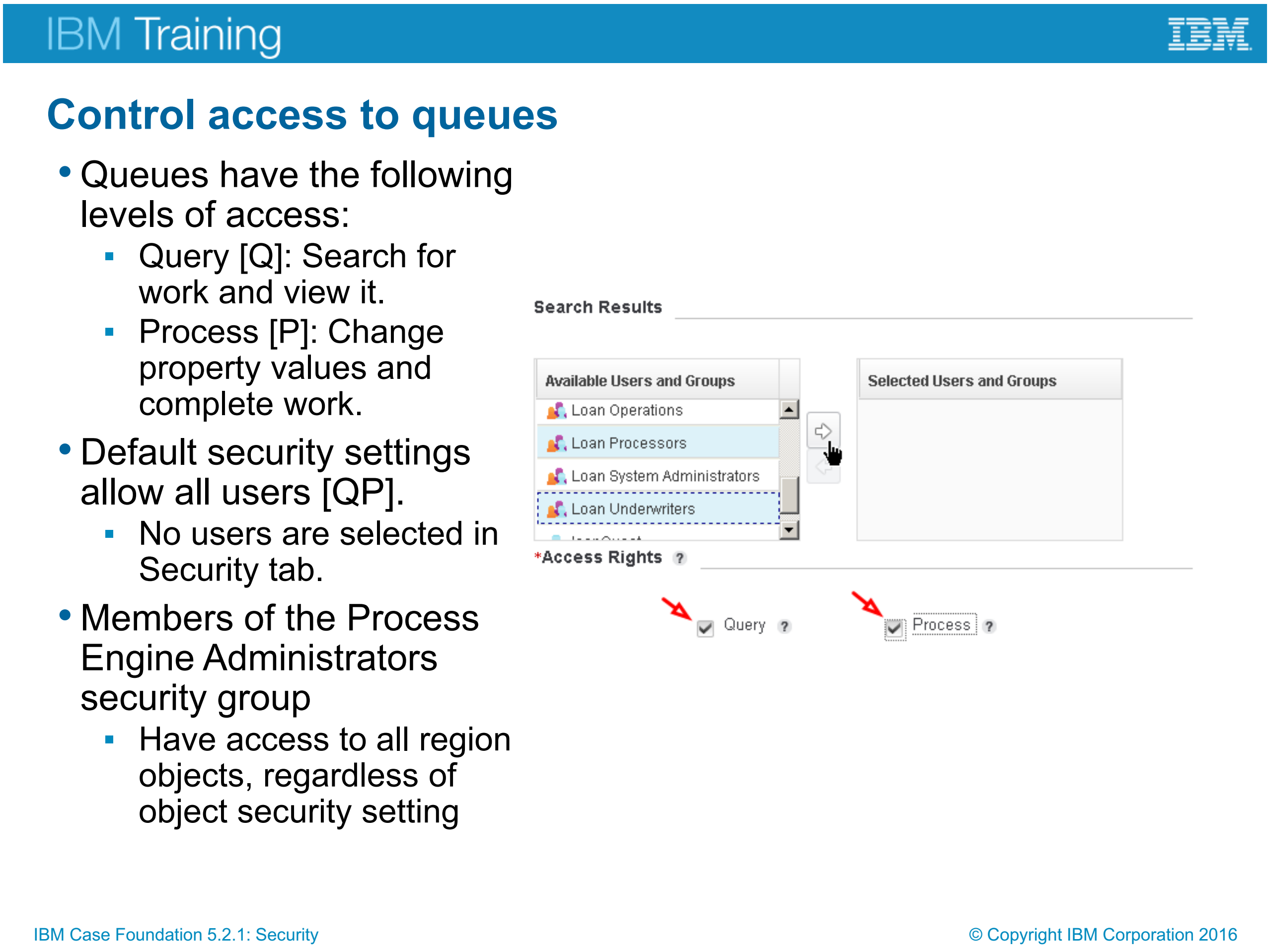
FileNet P8 Platform 5.2.0>Integrating workflow into document management>Configuring the workflow system>Getting started with Process Configuration Console>Security considerations for modifying the workflow configuration

> http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.0/com.ibm.p8.pe.configui.doc/bpfc046.htm

FileNet P8 Platform 5.2.1>Administering>Administering Content Platform Engine>Defining the workflow system>Configuring the workflow system>Managing the workflow system>Assigning workflow security levels

> http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.ce.admin.tasks.doc/p8pcc303.htm

By default, roster, queue, and event log access is unrestricted. To secure access, assign at least one user to each possible access right for the roster or queue. For example, to prevent all users from accessing a queue, assign the Query and Process access right to one member of the Process Engine Administrator Group, which already has implicit access to the queue.



IBM Training

Control access to queues

- Queues have the following levels of access:
  - Query [Q]: Search for work and view it.
  - Process [P]: Change property values and complete work.
- Default security settings allow all users [QP].
  - No users are selected in Security tab.
- Members of the Process Engine Administrators security group
  - Have access to all region objects, regardless of object security setting

IBM Case Foundation 5.2.1: Security

Figure 1-22. Control access to queues

Help path

FileNet P8 Platform 5.2.1>Security>Authorization>Object access rights and security>Workflow rosters and queues

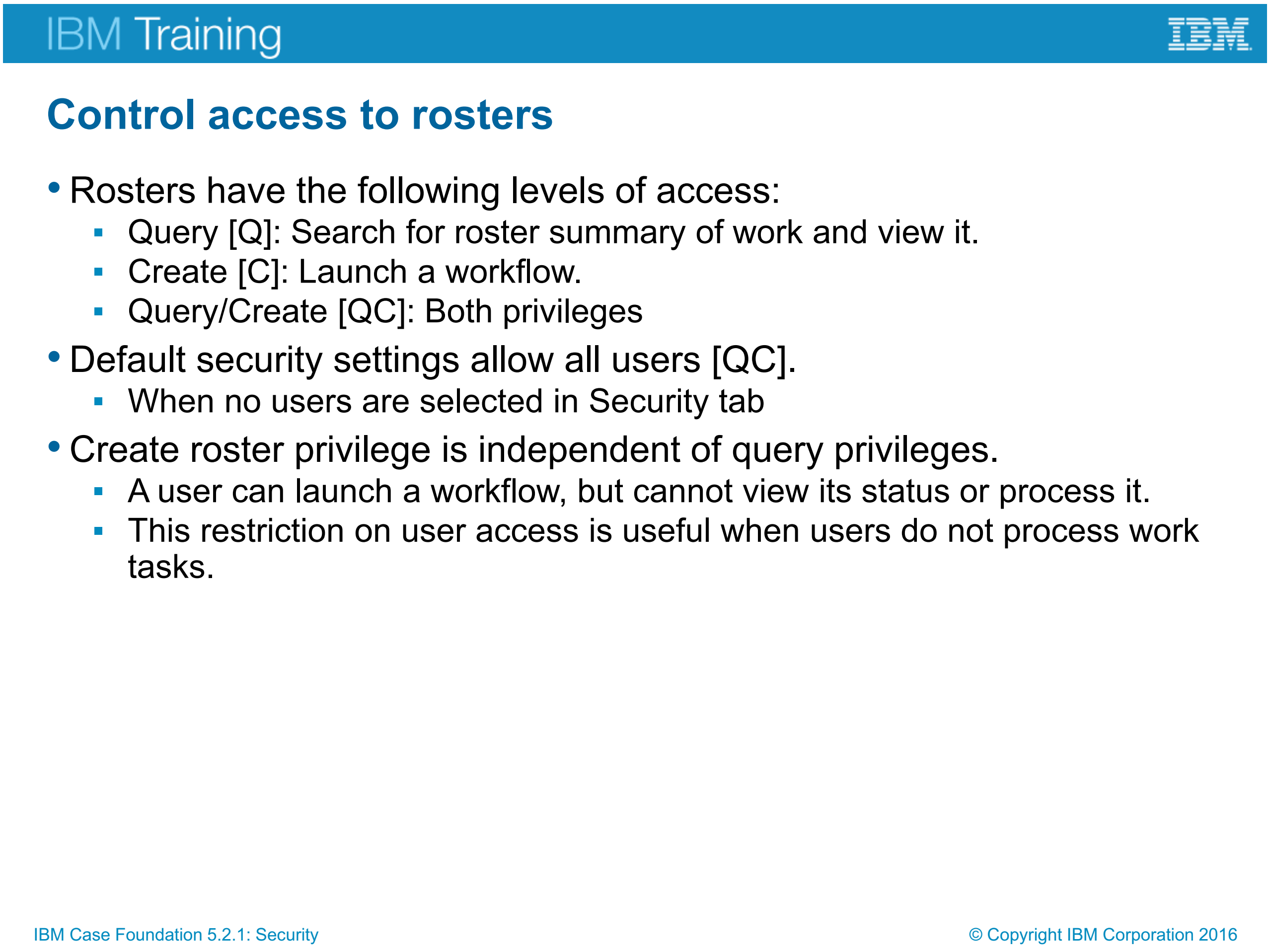
> http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psa012.htm

If a user is a member of the Workflow System Administrator Group, the user automatically has full rights to each roster and queue, even if the user is not explicitly assigned access rights. A user must have query access to a queue in order to be able to process it.

If a user does not have at least Query access to a work queue, the user cannot see the queue.

The combination of queue and roster privileges for a user affects how that user can use process applications.

The screen capture shows an example of the interface that is used to add users and groups to a queue.



IBM Training

Control access to rosters

- Rosters have the following levels of access:
  - Query [Q]: Search for roster summary of work and view it.
  - Create [C]: Launch a workflow.
  - Query/Create [QC]: Both privileges
- Default security settings allow all users [QC].
  - When no users are selected in Security tab
- Create roster privilege is independent of query privileges.
  - A user can launch a workflow, but cannot view its status or process it.
  - This restriction on user access is useful when users do not process work tasks.

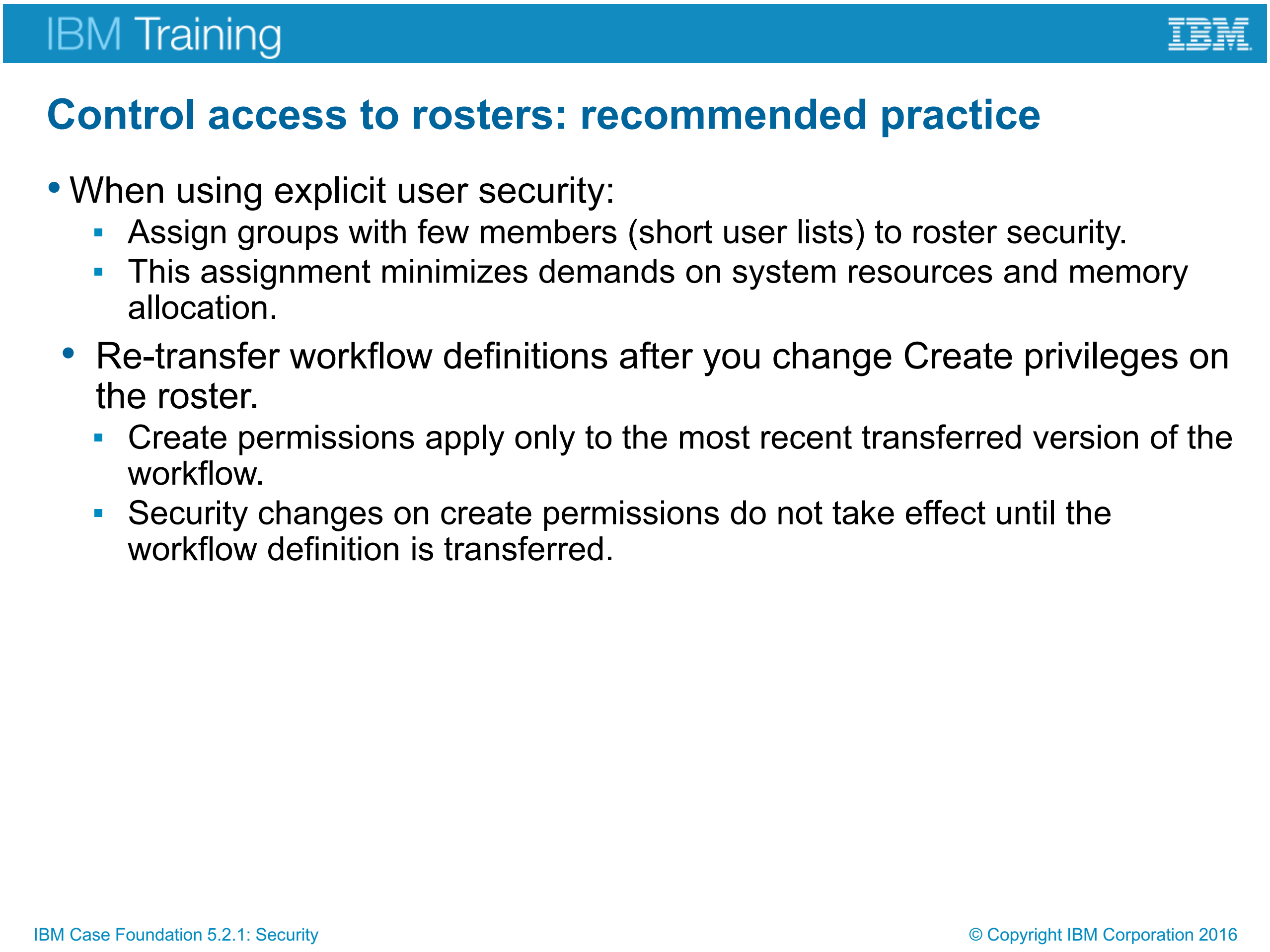
IBM Case Foundation 5.2.1: Security

© Copyright IBM Corporation 2016

Figure 1-23. Control access to rosters

Help path

Unlike the Process privilege in queues, the Create privilege in rosters is not dependent on query privileges. A user can launch a workflow without permission to view it later. This restriction is useful for cases in which users do not have a role in processing the work. For example, a customer who emails a comment about the loan process might trigger a workflow to handle the comment, but the customer has no role in the workflow and no need to view the workflow.



IBM Training

Control access to rosters: recommended practice

- When using explicit user security:
  - Assign groups with few members (short user lists) to roster security.
  - This assignment minimizes demands on system resources and memory allocation.
- Re-transfer workflow definitions after you change Create privileges on the roster.
  - Create permissions apply only to the most recent transferred version of the workflow.
  - Security changes on create permissions do not take effect until the workflow definition is transferred.

IBM Case Foundation 5.2.1: Security

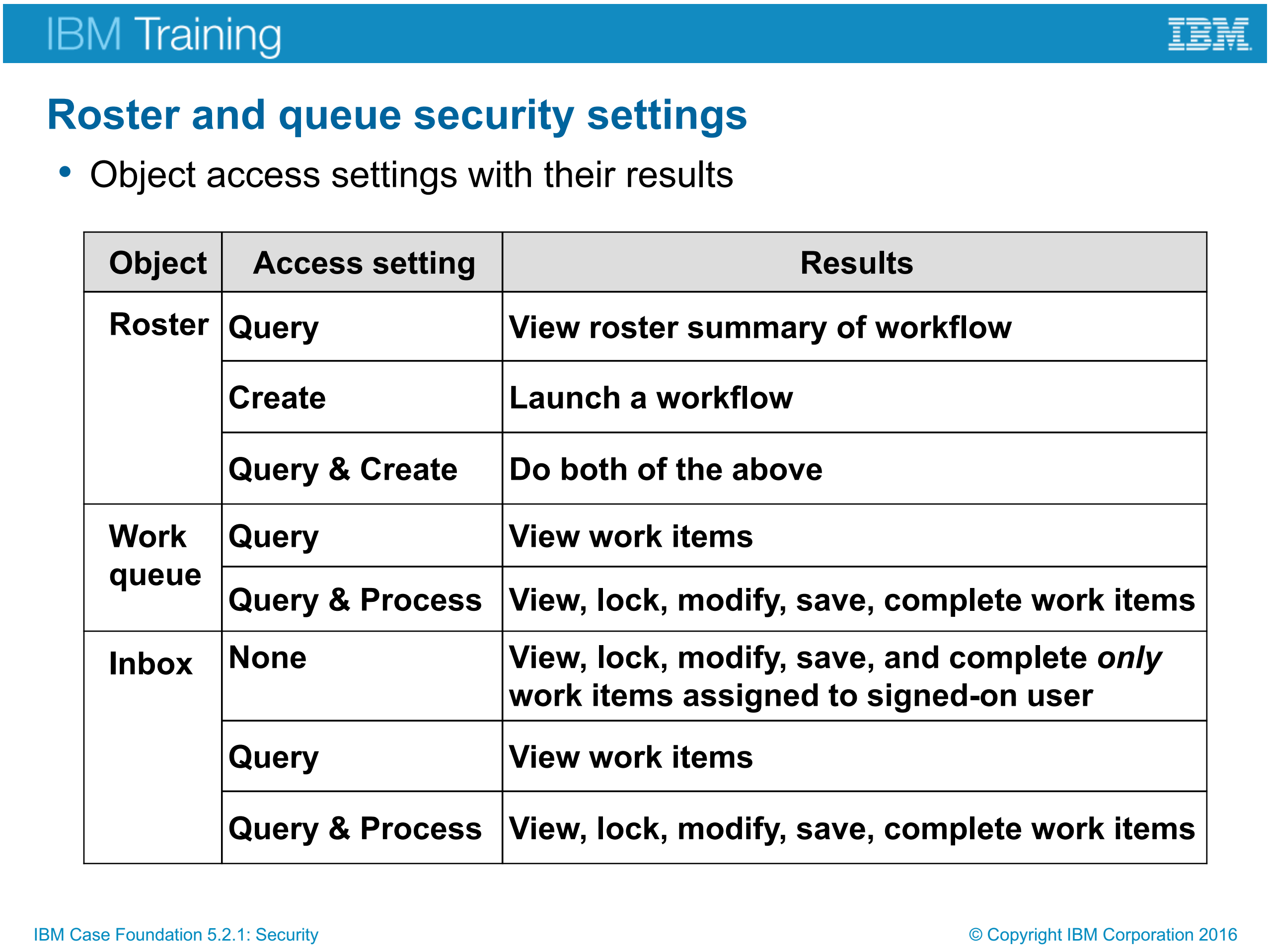
© Copyright IBM Corporation 2016

Figure 1-24. Control access to rosters: recommended practice

When you set explicit user security, do not assign groups with many members or large lists of users to roster security because large assignments make extra demands on system resources and memory allocation.

Determine who needs to access information regarding a particular workflow. The answer is typically administrators and the manager for the work that is being processed.

Several versions of a workflow can run simultaneously. The workflow and the process region configuration are saved at the time that the workflow definition is transferred. The benefit to this model is that you can continue to run prior versions of workflows even after newer versions are transferred. For example, in a development environment, you can complete workflows that were started before the workflow was updated. Without this capability, the older workflows might go into an error state. When you change the Create permission on the roster, you need to retransfer the workflow definition so that the workflow configuration information is updated to reflect the changes.



IBM Training

Roster and queue security settings

- Object access settings with their results

Object	Access setting	Results
Roster	Query	View roster summary of workflow
	Create	Launch a workflow
	Query & Create	Do both of the above
Work queue	Query	View work items
	Query & Process	View, lock, modify, save, complete work items
Inbox	None	View, lock, modify, save, and complete *only* work items assigned to signed-on user
	Query	View work items
	Query & Process	View, lock, modify, save, complete work items

IBM Case Foundation 5.2.1: Security

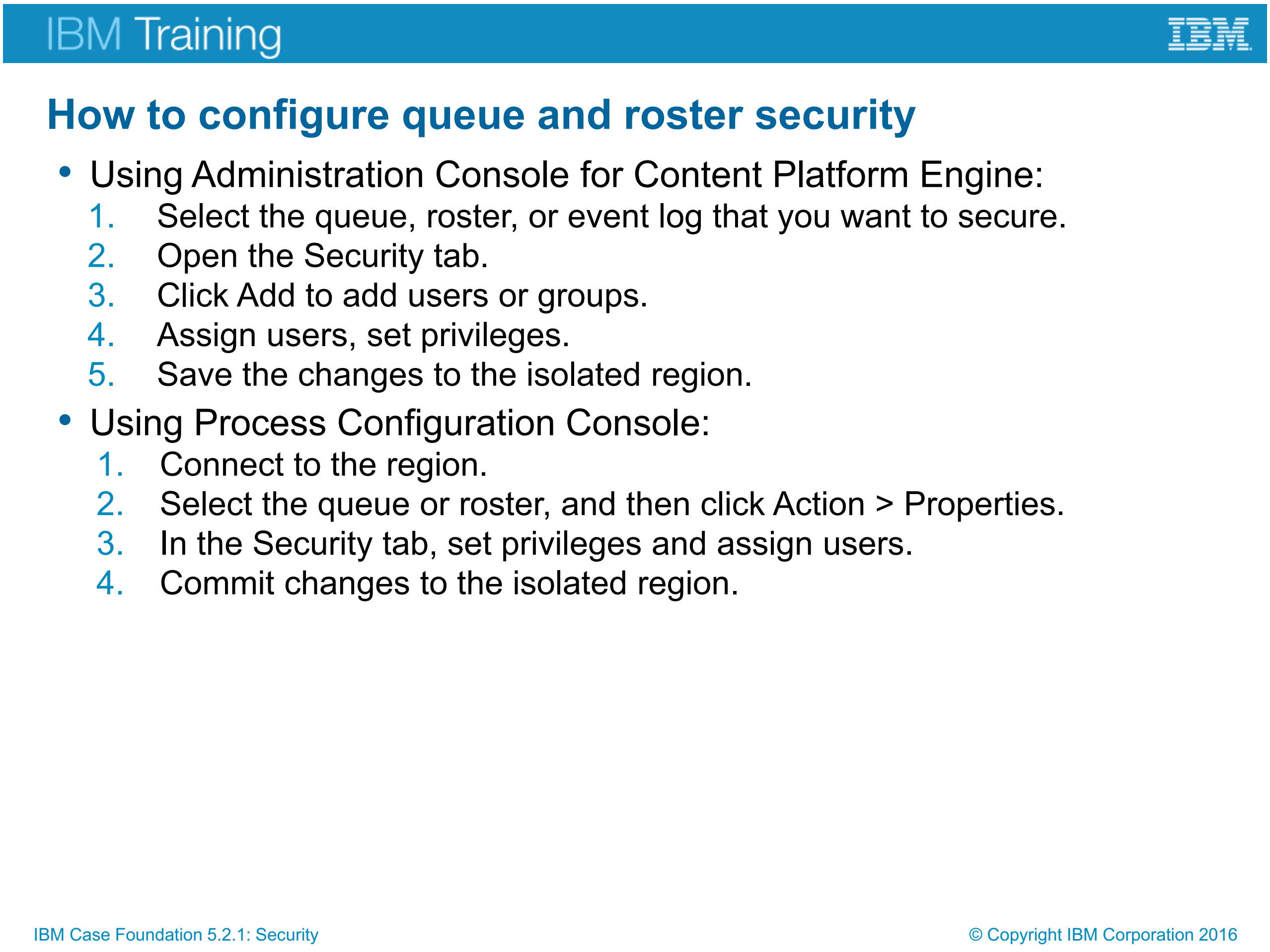
© Copyright IBM Corporation 2016

Figure 1-25. Roster and queue security settings

Help path

FileNet P8 Platform 5.2.1>Integrating workflow into document management>Process applications concepts>Administration and configuration>Workflow security

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.pe.user.doc/bpfcg005.htm



IBM Training

How to configure queue and roster security

- Using Administration Console for Content Platform Engine:
  1. Select the queue, roster, or event log that you want to secure.
  2. Open the Security tab.
  3. Click Add to add users or groups.
  4. Assign users, set privileges.
  5. Save the changes to the isolated region.
- Using Process Configuration Console:
  1. Connect to the region.
  2. Select the queue or roster, and then click Action > Properties.
  3. In the Security tab, set privileges and assign users.
  4. Commit changes to the isolated region.

IBM Case Foundation 5.2.1: Security

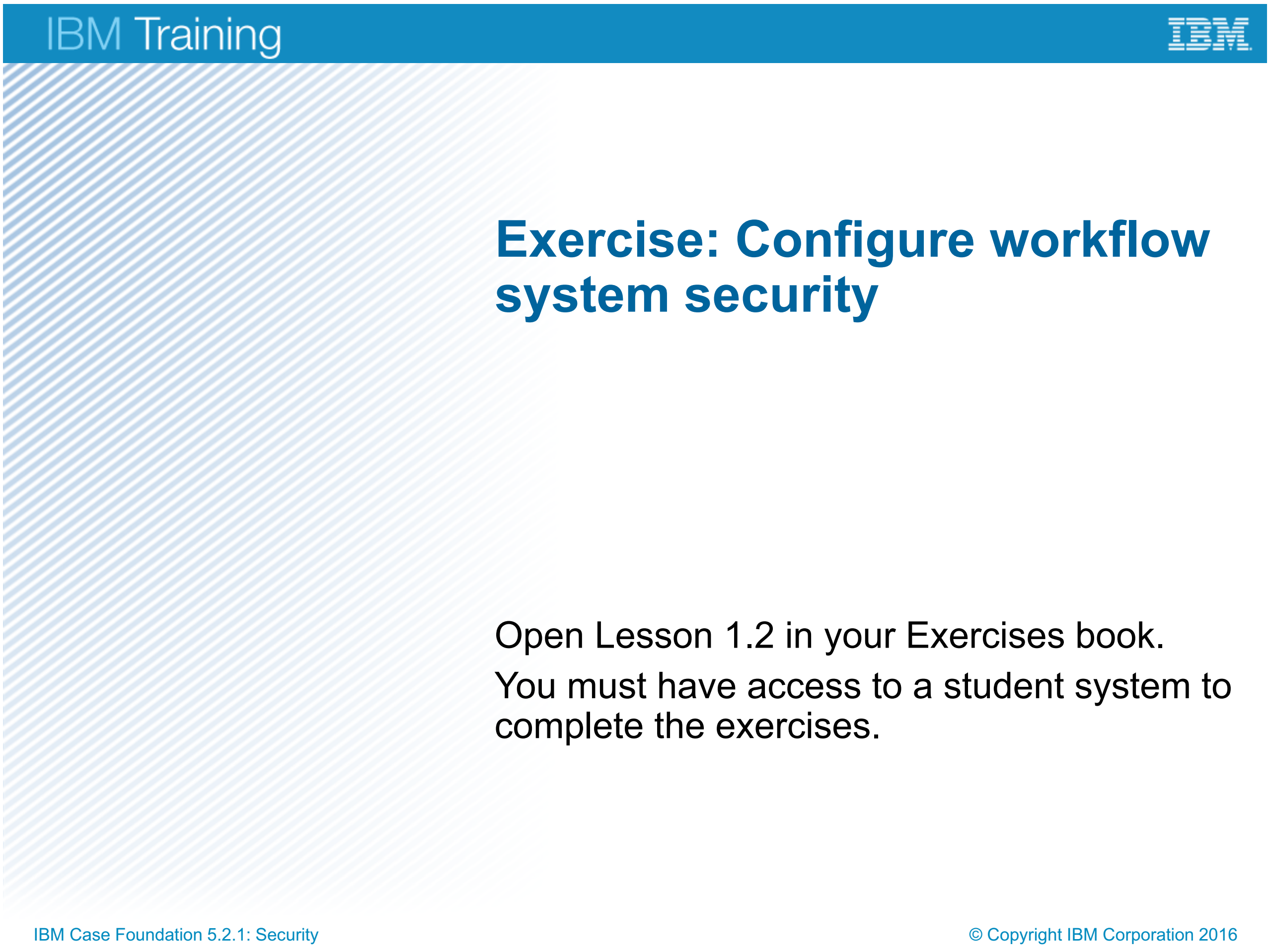
© Copyright IBM Corporation 2016

Figure 1-26. How to configure queue and roster security

Help path

FileNet P8 Documentation > User Help > Integrating workflow > Workflow applications > Process Configuration Console > Getting Started > Manage properties of queues, rosters, and event logs > Set security levels

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.pe.configui.doc/bpfc019.htm



IBM Training

Exercise: Configure workflow system security

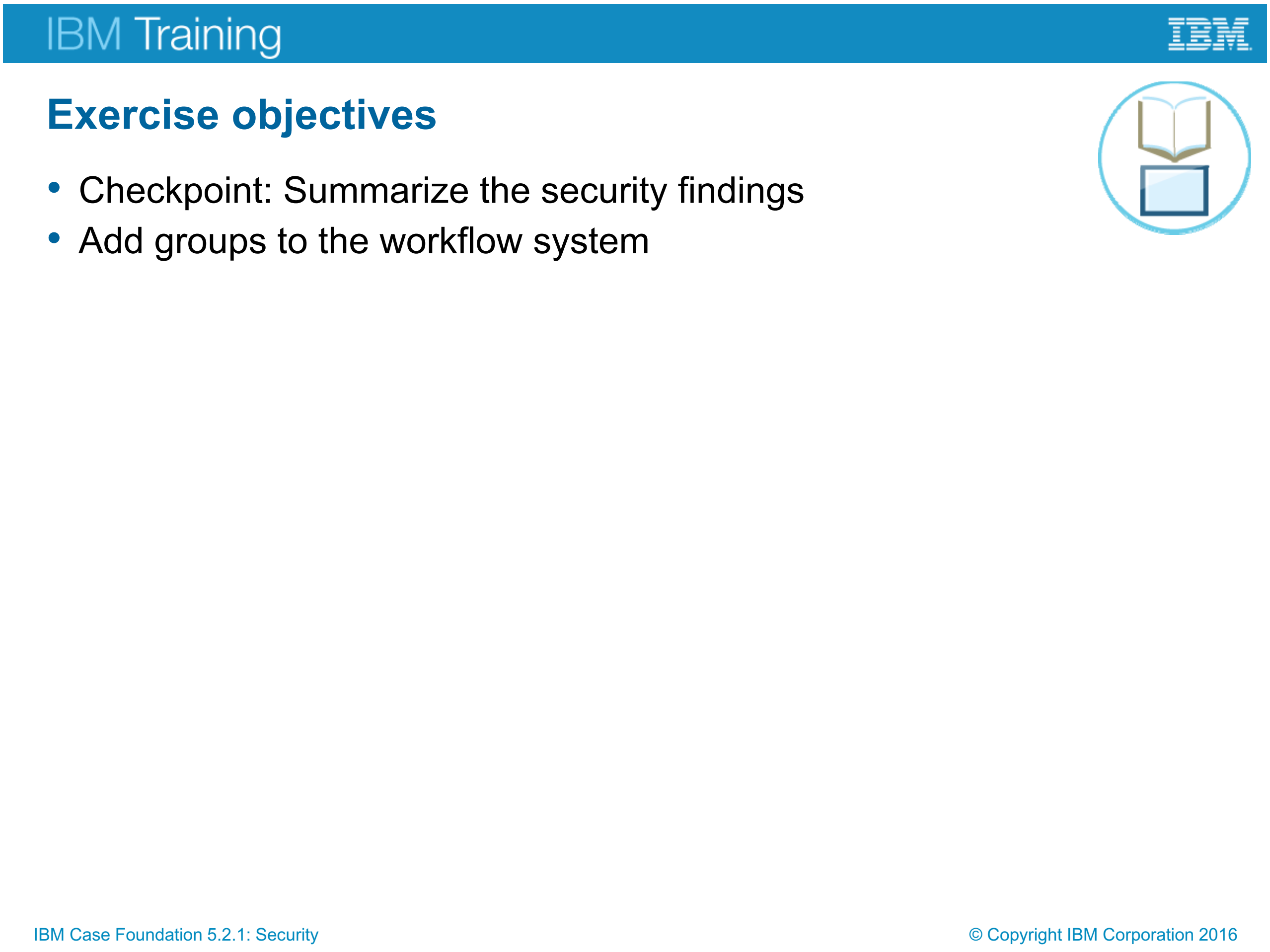
Open Lesson 1.2 in your Exercises book.

You must have access to a student system to complete the exercises.

IBM Case Foundation 5.2.1: Security

© Copyright IBM Corporation 2016

Figure 1-27. Exercise: Configure workflow system security



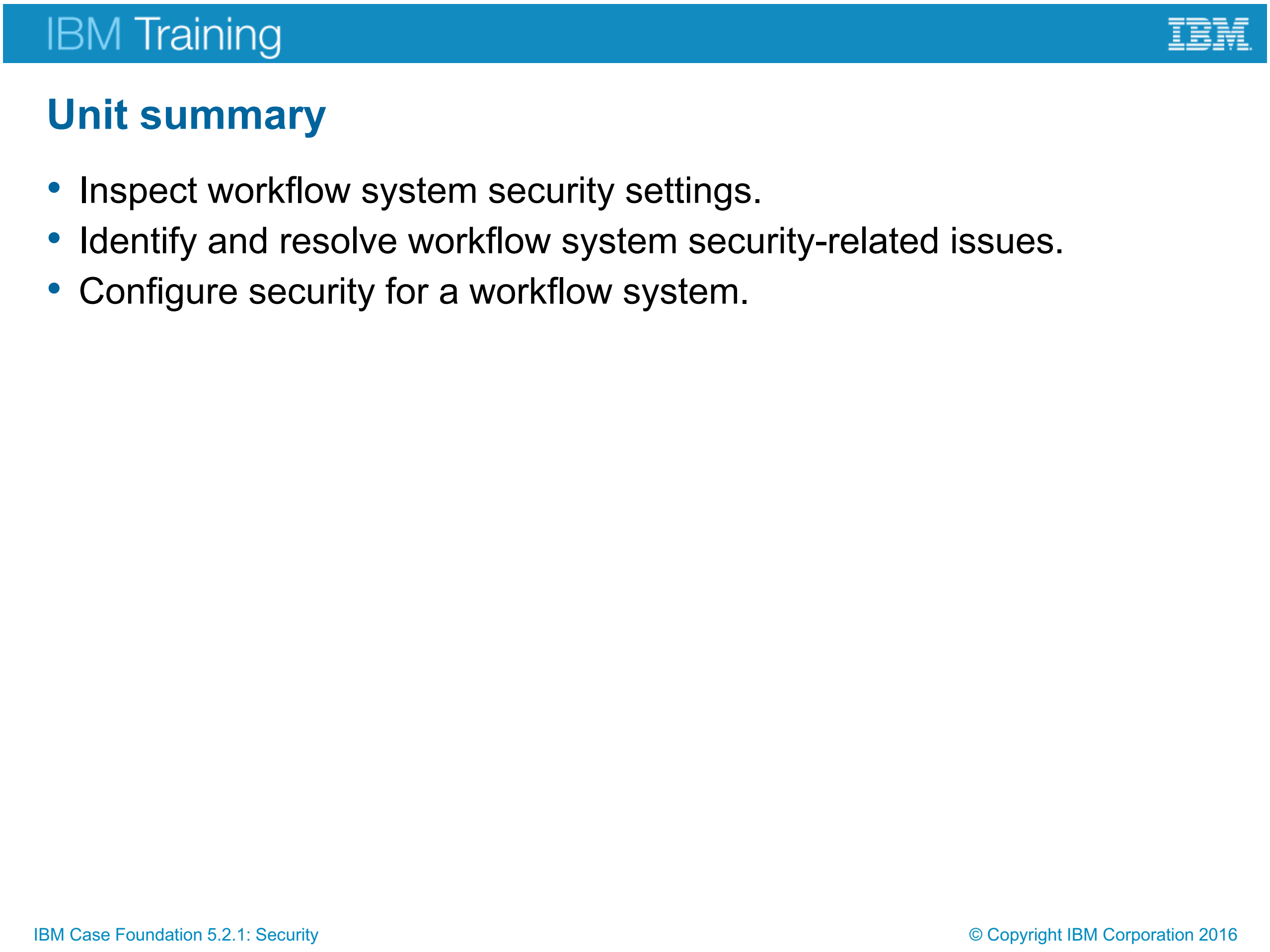
IBM Training

Exercise objectives

- Checkpoint: Summarize the security findings
- Add groups to the workflow system

IBM Case Foundation 5.2.1: Security

Figure 1-28. Exercise objectives



IBM Training

Unit summary

- Inspect workflow system security settings.
- Identify and resolve workflow system security-related issues.
- Configure security for a workflow system.

IBM Case Foundation 5.2.1: Security

© Copyright IBM Corporation 2016

Figure 1-29. Unit summary

IBM Training