IBM Security Identity Governance and Intelligence
Version 5.2.2

Scenarios Topics

IBM Security Identity Governance and Intelligence
Version 5.2.2

Scenarios Topics

Table of contents

Table list

Chapter 1. Scenarios overview

The following scenarios describe some of the common activities that users and administrators do in IBM® Security Identity Governance and Intelligence to configure the environment and complete daily tasks.

The scenarios demonstrate how company administrators, managers, and employees use Identity Governance and Intelligence to provision users into Identity Governance and Intelligence and do common identity and governance activities. These scenarios are grouped by the type of user who does the activity. Identity Governance and Intelligence provides views for these common user types:

Virtual appliance administrators
Virtual appliance administrators perform tasks in the virtual appliance.

Identity Governance and Intelligence administrators
Identity Governance and Intelligence administrators perform tasks in the Administration Console.

Business users
Business users perform tasks in the various dashboards of the Service Center, depending on their access and responsibilities.

- Application managers
- User managers
- Role managers
- Risk managers
- Help desk personnel
- Employees

The scenarios are only a subset of activities that these user types do, but they highlight some of the capabilities that Identity Governance and Intelligence offers.

For more information about the users and tasks, see Roadmap of personas and tasks.

Chapter 2. Importing and mapping account attributes for HR feed profiles

This scenario provides a high-level view of the procedures for importing an HR feed adapter profile and importing the attributes into the Identity Governance and Intelligence data model.

Table 1. Procedures for importing and mapping account attributes for HR feed profiles

Procedure	**For more information**
Consult the documentation for your HR feed adapter to define the attribute map for your adapter profile.	• PeopleSoft HR feed adapter Installation and Configuration Guide • SAP HR feed adapter Installation and Configuration Guide
Configure the rule for the unique user ID.	Configuring the rule for the unique user ID
Import an HR feed target type (adapter profile).	Importing HR feed adapter profiles
Import the attribute map from your HR feed adapter profile into Identity Governance and Intelligence.	Importing the attribute map for a target type
Create a target instance.	Creating targets to support HR feed
Reconcile the data.	Reconciling accounts immediately on a target

Chapter 3. Role mining to isolate the best roles

The IT security department wants to reduce the volume of activities for a company-wide certification campaign. It conducts a role mining session to isolate the best roles that are embedded in the organization.

Before you begin

Role mining is done on a production system on which you already modeled the solution and deployed the customer contents that are mapped on the Identity Governance and Intelligence data model. Therefore, you must already have a system with OUs, users, entitlements, and other elements. You must load data in the role mining database schema. After you meet these conditions, you can start role mining.

Note: Role mining can occur at any time, typically when the system is in production for some time and is fed with significant data. Therefore, some customers might not immediately employ role mining activities. For example, if you did not adopt role-based access control before you deployed Identity Governance and Intelligence, you might not use role mining functions for the first period in the production environment. Use this time to gather data to determine how to include role engineering activity.

This scenario requires someone who is both an expert in Identity Governance and Intelligence functions and who is well-versed in customer context and processes. Typically, this person is an administrator and an expert manager of the customer who is trained on software functions and the data model.

After role mining, you can select a role and see it visualized as a map. Understanding the map information requires training that is centered on the analysis of the map. See the following resources:

- Maps
- Candidate Roles

About this scenario

Identity Governance and Intelligence is based on the role-based access control standard so you can better implement governance policies of governance if you model the system permissions into roles.

In a business setting, roles are defined according to job competency, authority, and responsibility.

Role mining is the process of analyzing user-to-resource mapping data to determine or modify user permissions for role-based access control in an enterprise. Role mining is the best way to aggregate existing user permissions, or entitlements, into a role.

If you can collapse 100 permissions into a role, you can assign that role to users with only one assignment instead of making 100 assignments of 100 permissions. If you model the system according to role-based access control, you have all advantages of that approach.

Use role mining to help you determine the best roles for:

- Optimizing the Access Certifier activity to model a Certification Campaign.
- Optimizing the Segregation of Duties functions if you implement SoD.
- Testing the behavior of the system if you modify the dataset contents, which is mainly, but not limited to, the set of users and permissions.

In this scenario, you use the following features of Identity Governance and Intelligence:

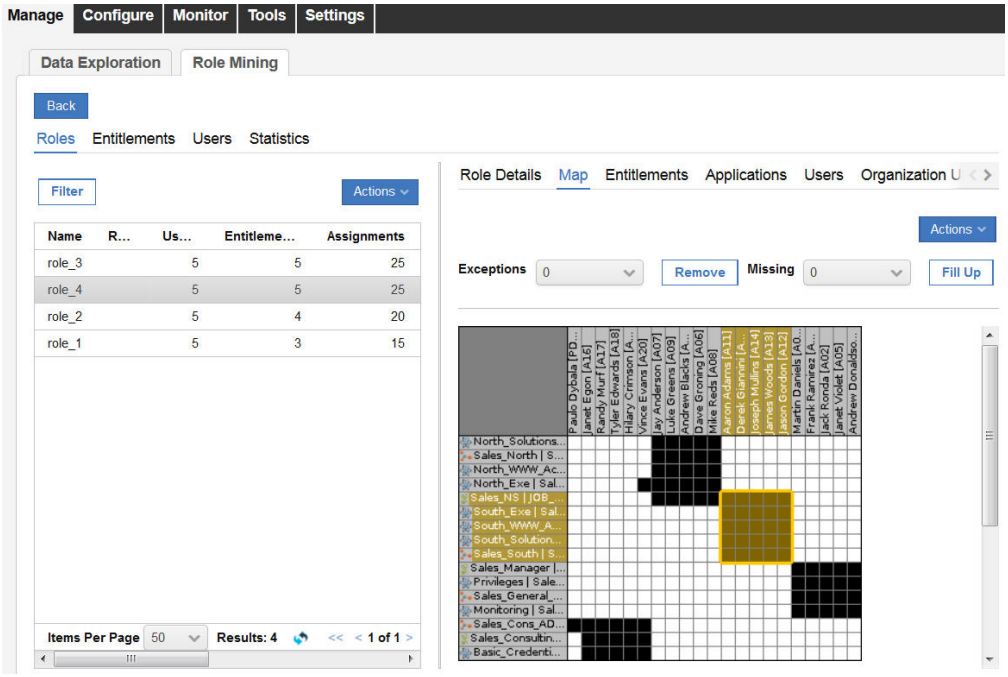
- Role mining
- Roles

For the following workflow, you are the Engineer of Roles. You suspect that you might have too many entitlements that are assigned to users, and they are not well-grouped. You want to find all candidate roles with the following characteristics:

- A minimum of two users per role
- A minimum of two entitlements per role
- Related to a specific organization
- Related to the entitlement of a specific application, such as Active Directory
- Has only direct assignments
- A parameter for setting the role mining, which in this case is **`Balanced coverage and commonality`**

Workflow

1. Log in to the Administration Console. Use the default credentials.
2. Click **Access Optimizer**.
3. Click **Manage** > **Role Mining** > **Actions** > **Add**.
4. Start a new role mining configuration in the New Role Mining window.
   a. Enter 2 at **Minimum Number of Users per Role**.
   b. Enter 2 at **Minimum Number of Entitlements per Role**.
   c. Select an organizational unit at **Org Unit**.
   d. Select an application at **Application**.
   e. Use the default values for all other options.
   f. Click **Ok**.
5. Wait for the status icon to turn green.
6. Click **Manage** > **Role Mining**.
7. Click the magnifying glass icon.
8. Select the **Roles** tab. The **Roles** tab lists the suggested roles that are based on the previous analysis (see steps 1 - 5).
9. Select a role (in the following example, **role_4**).
10. Click **Manage** > **Role Mining** > **Roles** > **Map** to investigate the map **user-entitlements**, which is highlighted by the yellow box.



Note: The role mining engine automatically names the roles **role_1**, **role_2**, **role_#**, which are not useful for a quick identification.

11. If this role is useful for your purpose, you can rename **role_4** and import it into Access Governance Core.
    a. Click **Manage** > **Role Mining** > **Roles** > **Impact Analysis**.
    b. In the central frame, select the item that is related to the selected **role_4**.
    c. Click **Actions** > **Release to AGC**.
    d. In the **Release** window, set a meaningful name (for example, `AD common role for North`).
    e. Click **Ok**.
12. Click the application menu, and then select **Access Governance Core**.
13. In the **Manage** > **Roles** tab, select the role `AD common role for North` that was just released.
14. Click **Manage** > **Roles** > **Actions** > **Publish** to make the new role available.
15. Click **Manage** > **Roles** > **Actions** > **Consolidate**.

    Note: The consolidation process loads the users from the old role into the new role.

What to do next

You can now assign this role to other users.

Index

Printed in USA